

IBM Rational Developer for System z
Versão 9.1.1

*Guia de Referência de Configuração do
Host*



IBM Rational Developer for System z
Versão 9.1.1

*Guia de Referência de Configuração do
Host*



Observação

Antes de usar estas informações, certifique-se de ler as informações gerais em “Avisos” na página 221.

Nona Edição (Dezembro de 2014)

Esta edição aplica-se ao IBM Rational Developer for System z Versão 9.1.1 (número do programa 5724-T07) e a todas as liberações e modificações subsequentes até indicado de outra forma em novas edições.

Solicite as publicações pelo telefone ou fax. O IBM Software Manufacturing Solutions recebe os pedidos de publicações entre 8h30 e 19h, horário padrão na costa leste dos Estados Unidos. O número de telefone é (800) 879-2755. O número de fax é (800) 445-9269. O fax deve ser enviado para: Publications, 3rd floor.

Você também pode solicitar as publicações por meio de um representante IBM ou da filial da IBM que atende em sua região. As publicações não são guardadas no endereço a seguir.

A IBM agradece pelo seu comentário. Você pode enviar os comentários por correio ao seguinte endereço:

IBM Brasil - Centro de Traduções
Rodovia SP 101 Km 09
Rodovia SP 101 Km 09
CEP 13185-900
Hortolândia, SP

É possível enviar um fax com os seus comentários para: 1-800-227-5088 (Estados Unidos e Canadá)

Ao enviar informações à IBM, você concede à IBM o direito não exclusivo de utilizar ou distribuir as informações da forma que julgar apropriada, sem incorrer em qualquer obrigação para com o Cliente.

Nota para Usuários do Governo dos Estados Unidos - Uso, duplicação ou divulgação restritos pelo documento GSA ADP Schedule Contract com a IBM Corp.

© Copyright IBM Corporation 2000, 2014.

Conteúdo

| | |
|----------------|------------|
| Figuras | vii |
|----------------|------------|

| | |
|----------------|-----------|
| Tabelas | ix |
|----------------|-----------|

| | |
|-----------------------------|-----------|
| Sobre este Documento | xi |
|-----------------------------|-----------|

| | |
|---|-----|
| Quem Deve Usar este Documento | xii |
| Resumo das Mudanças | xii |
| Descrição do Conteúdo do Documento | xiv |
| Entendendo o Developer for System z | xiv |
| Considerações de segurança | xiv |
| Considerações de TCP/IP | xiv |
| Considerações WLM | xv |
| Considerações de Ajuste | xv |
| Considerações sobre Desempenho | xv |
| Considerações de Push-to-client | xv |
| considerações CICSTS | xv |
| Considerações da Saída de Usuário | xv |
| Customizando o Ambiente TSO | xv |
| Executando várias instâncias | xv |
| Resolução de problemas de configuração | xvi |
| Configurando o SSL e a Autenticação X.509 | xvi |
| Configurando o TCP/IP | xvi |

Guia de Referência de Configuração do Host do IBM Rational Developer for System z

Capítulo 1. Entendendo o Developer for System z

| | |
|--|----|
| Visão geral do componente | 3 |
| RSE como um aplicativo Java | 5 |
| donos das tarefas | 6 |
| Fluxo de conexão | 8 |
| Depurador Integrado | 10 |
| CARMA | 10 |
| Arquivos de Configuração CARMA | 11 |
| CRASTART | 12 |
| Envio em Lote | 12 |
| Proprietário de Bloco de Conjunto de Dados | 13 |
| Liberando um Bloqueio | 14 |
| Estrutura de diretório do z/OS UNIX | 15 |
| Atualizar Privilégios para Administradores que | |
| Não São de Sistema | 17 |
| Comandos de Segurança Úteis | 17 |
| Comandos Úteis do z/OS UNIX | 17 |
| Configuração de Amostra | 18 |

Capítulo 2. Considerações de segurança

| | |
|-----------------------------|----|
| Métodos de autenticação | 20 |
| ID do Usuário e Senha | 20 |
| ID do Usuário e Senha Única | 20 |
| ID do usuário e passphrase | 20 |

| | |
|--|----|
| Certificado X.509 | 20 |
| Autenticação do JES Job Monitor | 20 |
| Autenticação do Debug Manager | 21 |
| Segurança de conexão | 21 |
| Limitar Comunicação Externa a Portas | |
| Especificadas | 22 |
| Criptografia de Comunicação Usando SSL ou TLS | 22 |
| Verificação de Port Of Entry | 23 |
| Usando os PassTickets | 23 |
| Criação de Log de Auditoria | 24 |
| Controle de Auditoria | 24 |
| Processamento de Auditoria | 25 |
| Dados de Auditoria | 25 |
| Segurança do JES | 26 |
| Ações nas Tarefas - Limitações de Destino | 26 |
| Ações nas Tarefas - Limitações de Execução | 27 |
| Acesso aos Arquivos de Spool | 29 |
| Comunicação Criptografada de SSL/TLS | 29 |
| Comunicação Criptografada pelo Depurador Integrado | 31 |
| Autenticação de cliente usando certificados X.509 | 31 |
| Validação da Autoridade de Certificação (CA) | 32 |
| (Opcional) Consulte uma Certificate Revocation List (CRL) | 32 |
| Autenticação por Software de Segurança | 33 |
| Autenticação por Daemon do RSE | 34 |
| Verificação de Port Of Entry (POE) | 34 |
| Alterando Funções de Cliente | 35 |
| OFF.REMOTECPY.MVS | 36 |
| Grupos de Desenvolvedores de Push-to-client | 36 |
| Segurança do arquivo de log | 37 |
| Permissões de classe UNIXPRIV | 39 |
| Permissão do perfil BPX.SUPERUSER | 39 |
| UID 0 | 39 |
| Segurança de Depuração | 40 |
| segurança do CICSTS | 40 |
| repositório do CRD | 40 |
| transações do CICS | 41 |
| comunicação criptografada por SSL | 41 |
| Segurança de SCLM | 41 |
| Informações Variadas | 41 |
| Lixeira GATE | 41 |
| ACEE Gerenciado | 41 |
| Armazenamento em cache do ACEE | 42 |
| arquivos de configuração do Developer for System z | 42 |
| JES Job Monitor - FEJJCNGF | 42 |
| RSE - rsed.envvars | 42 |
| RSE - ssl.properties | 44 |
| RSE - pushtoclient.properties | 44 |
| Definições de segurança | 44 |
| Requisitos e Lista de Verificação | 45 |
| Ativar Configurações de Segurança e Classes | 46 |
| Definir um segmento OMVS para usuários do Developer for System z | 47 |

| | | | |
|--|-----------|--|------------|
| Definir as Tarefas Iniciadas do Developer for System z | 47 | Uso do espaço do sistema de arquivos z/OS UNIX | 98 |
| Definir RSE como um servidor z/OS UNIX seguro | 48 | Definições de Recursos Principais | 100 |
| Definir as Bibliotecas Controladas por Programa do MVS para RSE | 49 | /etc/rdz/rsed.envvars | 100 |
| Definir Suporte de PassTicket para RSE | 50 | SYS1.PARMLIB(BPXPRMxx) | 101 |
| Defina a permissão de acesso do arquivo z/OS UNIX para RSE | 51 | Várias definições de recurso | 104 |
| Definir a Proteção do Aplicativo para RSE | 51 | Placa EXEC na JCL do Servidor | 104 |
| Definir os Arquivos Controlados por Programa do z/OS UNIX para RSE | 52 | FEK.#CUST.PARMLIB(FEJJCNFG) | 104 |
| Definir a Segurança de Comando JES. | 52 | SYS1.PARMLIB(IEASYSxx) | 105 |
| Definir acesso ao depurador integrado | 54 | SYS1.PARMLIB(IVTPRMxx) | 105 |
| Definir Perfis de Conjuntos de Dados. | 54 | SYS1.PARMLIB(ASCHPMxx) | 105 |
| Verifique as Configurações de Segurança | 58 | Monitoramento | 106 |
| Capítulo 3. Considerações de TCP/IP | 61 | Monitoramento de RSE | 106 |
| Portas TCP/IP | 61 | Monitorando o z/OS UNIX | 107 |
| Comunicação Externa | 62 | Monitorando da Rede. | 108 |
| Comunicação interna | 62 | Monitorando Sistemas de Arquivos z/OS UNIX | 108 |
| Reserva de Porta TCP/IP. | 63 | Configuração de Amostra | 109 |
| portas do CARMA e TCP/IP | 63 | Contagem do Conjunto de Encadeamento | 109 |
| Considerações de LDAP | 63 | Determinar Limites Mínimos | 109 |
| Substituindo o Comportamento TCP/IP Padrão | 64 | Definindo Limites | 110 |
| ACK Atrasado | 64 | Uso de Recurso de Monitor. | 111 |
| Multipilhas (CINET) | 64 | Capítulo 6. Considerações sobre Desempenho. | 113 |
| O CARMA e a Afinidade de Pilha | 65 | Usar Sistemas de Arquivos zFS | 113 |
| crastart*.conf | 65 | Evite o Uso de STEPLIB. | 113 |
| CRASUB* | 65 | Aprimorar o acesso às bibliotecas do sistema | 113 |
| Distributed Dynamic VIPA | 65 | Bibliotecas de Tempo de Execução Language Environment (LE) | 114 |
| Restringindo a Seleção de Portas | 67 | Desenvolvimento de Aplicativos | 114 |
| Configuração de Amostra. | 68 | Aprimorando o desempenho da verificação de segurança | 115 |
| Sistema SYS1 – Perfil TCP/IP | 69 | Gerenciamento de carga de trabalho. | 115 |
| Sistema SYS2 – Perfil TCP/IP | 69 | Tamanho de heap Java fixo | 115 |
| Capítulo 4. Considerações WLM. | 71 | Opção Java -Xquickstart | 116 |
| Classificação de Carga de Trabalho | 71 | Compartilhamento de Classe entre JVMs | 116 |
| Regras de Classificação | 72 | Ativar Compartilhamento de Classes | 116 |
| Configurando Objetivos | 73 | Limites de Tamanho de Cache. | 117 |
| Considerações para Seleção de Objetivos | 74 | Segurança do Cache | 117 |
| STC | 74 | SYS1.PARMLIB(BPXPRMxx) | 117 |
| OMVS | 75 | Espaço em disco | 118 |
| JES | 76 | Utilitários de Gerenciamento de Cache | 118 |
| ASCH | 77 | Capítulo 7. Considerações de Push-to-client | 119 |
| CICS | 77 | Introdução | 119 |
| Capítulo 5. Considerações de Ajuste | 79 | Sistema Primário | 120 |
| Uso de Recursos. | 79 | Metadados Push-to-client | 120 |
| Visão Geral (Overview) | 80 | Local de Metadados | 120 |
| Contagem do espaço de endereço | 81 | Segurança de Metadados | 121 |
| Contagem de processos | 83 | Uso de Espaço de Metadados | 122 |
| Contagem de encadeamentos | 86 | Controle de Configuração do Cliente | 122 |
| Uso temporário de recursos | 89 | Controle de Versão do Cliente | 123 |
| Contagem de encadeamentos | 90 | Diversos Grupos de Desenvolvedores | 123 |
| Uso de Armazenamento | 93 | Ativação | 123 |
| Limite de Tamanho de Heap Java | 93 | Concatenações de Grupo | 124 |
| Limite de Tamanho do Espaço de Endereço. | 94 | Ligação da Área de Trabalho | 124 |
| Diretrizes de Estimativa de Tamanho | 95 | Local de Metadados do Grupo | 125 |
| Análise do Uso de Armazenamento de Amostra | 96 | Etapas de Configuração | 126 |
| | | Seleção de Grupo Baseada em LDAP | 127 |
| | | Esquema LDAP | 128 |

| | |
|--|-----|
| Seleção do Servidor LDAP | 128 |
| Local do Servidor LDAP | 129 |
| Configuração de Amostra | 129 |
| Incluindo Backend push-to-client no LDAP | 130 |
| Configuração de Grupo LDAP Inicial | 130 |
| Incluir Desenvolvedores em Grupos LDAP | 131 |
| pushtoclient.properties | 131 |
| rsed.envvars. | 131 |
| /var/rdz/pushtoclient/*install | 131 |
| Seleção de Grupo Baseada em SAF | 132 |
| Configuração de Amostra | 133 |
| Definição de Segurança | 133 |
| pushtoclient.properties | 134 |
| rsed.envvars. | 134 |
| /var/rdz/pushtoclient/*install | 134 |
| Período de Carência para Rejeitar Mudanças | 134 |
| Projetos baseados no host | 135 |

Capítulo 8. considerações CICSTS 137

| | |
|---|-----|
| RESTful versus Serviços da Web | 138 |
| Regiões de Conexão Primária versus não primária | 138 |
| Log de Instalação de Recurso do CICS | 139 |
| segurança do Application Deployment Manager | 139 |
| segurança do repositório CRD. | 139 |
| Segurança de Pipeline | 139 |
| Segurança da Transação | 139 |
| comunicação criptografada por SSL | 140 |
| Segurança do Recurso | 141 |
| Administrative Utility | 141 |
| Notas de Migração do Utilitário Administrativo | 144 |
| Mensagens do Administrative Utility | 145 |
| Depuração de Transação do CICS | 147 |

Capítulo 9. Considerações da Saída de Usuário 149

| | |
|---|-----|
| Características da Saída de Usuário | 149 |
| Ativação da Saída de Usuário | 149 |
| Gravando uma Rotina de Saída do Usuário | 149 |
| Mensagens do console | 150 |
| Executando com um ID do Usuário da Variável | 150 |
| Shell Script do z/OS UNIX. | 150 |
| REXX exec do z/OS UNIX | 151 |
| Pontos de Saída Disponíveis | 151 |
| audit.action | 151 |
| logon.action | 152 |

Capítulo 10. Customizando o Ambiente TSO 153

| | |
|--|-----|
| O Serviço TSO Commands | 153 |
| Métodos de Acesso | 153 |
| Usando o Método de Acesso do TSO/ISPF Client Gateway | 154 |
| ISPF.conf | 154 |
| Usar Perfis do ISPF Existentes. | 154 |
| Usando um exec de alocação | 155 |
| Usar Diversos Execs de Alocação. | 155 |
| Diversos Arquivos ISPF.conf com Diversas Configurações do Developer for System z | 155 |

Capítulo 11. Executando várias instâncias 157

| | |
|--|-----|
| Configuração idêntica em um sysplex | 157 |
| Arquivos de Configuração Diferentes de Níveis de Software Idênticos. | 158 |
| Sincronização Automatizada | 159 |
| Todas as Outras Situações | 160 |

Capítulo 12. Resolução de problemas de configuração 163

| | |
|--|-----|
| Análise de Log e Configuração Usando FEKLOGS | 163 |
| Arquivos de Log | 164 |
| Criação de log do Debug Manager | 166 |
| criação de logs do JES Job Monitor | 166 |
| Criação de Log de Daemon RSE e de Conjunto de Encadeamento | 166 |
| criação de logs do usuário do RSE | 167 |
| criação de log do SCLM Developer Toolkit | 168 |
| Criação de logs do CARMA | 168 |
| Criação de Log IVP fekfivpc | 169 |
| Criação de log de teste IVP do fekfivpi. | 169 |
| Criação de Log de Teste IVP do fekfivps | 169 |
| Criação de Log da Revisão de Código | 169 |
| Criação de Log da Cobertura de Código | 169 |
| Arquivos de dump | 170 |
| Dumps do MVS | 170 |
| Dumps de Java. | 170 |
| Locais de Dump do z/OS UNIX | 171 |
| Rastreio | 172 |
| Rastreio do Debug Manager | 172 |
| rastreo do JES Job Monitor. | 172 |
| rastreo RSE | 172 |
| rastreo CARMA | 173 |
| Rastreio de feedback de erro | 173 |
| Bits de permissão do z/OS UNIX | 174 |
| atributo do sistema de arquivos SETUID | 175 |
| Autorização de controle de programa | 175 |
| Autorização APF | 176 |
| Sticky Bit. | 177 |
| Portas TCP/IP reservadas | 177 |
| Tamanho do espaço de endereço | 179 |
| Requisitos da JCL de Inicialização | 179 |
| Limitações Definidas em SYS1.PARMLIB(BPXPRMxx) | 179 |
| Limitações Armazenadas no Perfil de Segurança | 179 |
| Limitações Impostas por Saídas do Sistema | 179 |
| Limitações para Endereçamento de 64 Bits | 180 |
| Informações Variadas. | 180 |
| Encerramento Anormal por Falta de Espaço B37 de Feedback de Erro | 180 |
| Limites do sistema | 180 |
| Conexão recusada | 180 |
| OutOfMemoryError | 181 |
| Emulador de Conexão do Host | 181 |

Capítulo 13. Configurando o SSL e a Autenticação X.509 183

| | |
|--|-----|
| Decida Usar o SSL ou TLS Como o Método de Criptografia | 184 |
|--|-----|

| | |
|---|-----|
| Decidir Onde Armazenar Chaves Privadas e Certificados | 184 |
| Criar um Conjunto de Chaves com o RACF | 185 |
| Clonar a Configuração RSE Existente | 186 |
| Atualizar rsed.envvars para Ativar a Coexistência | 187 |
| Atualizar ssl.properties para Ativar SSL | 187 |
| Ativar SSL Criando um Novo Daemon RSE | 187 |
| Testar a Conexão | 188 |
| (Opcional) Incluir Suporte de Autenticação de Cliente X.509 | 191 |
| (Opcional) Criar um Banco de Dados de Chaves com gskkyman | 191 |
| (Opcional) Criar um Keystore com keytool | 193 |

Capítulo 14. Configurando o AT-TLS 195

| | |
|---|-----|
| Configurando syslogd | 196 |
| Configuração do AT-TLS no PROFILE.TCPIP | 196 |
| Tarefa Iniciada do Policy Agent | 196 |
| Configuração do Policy Agent | 197 |
| Política AT-TLS | 197 |
| Considerações sobre o TLS v1.2 | 199 |
| Atualizações de Segurança do AT-TLS | 199 |
| Ativação da Política AT-TLS | 201 |

Capítulo 15. Configurando o TCP/IP 203

| | |
|---------------------------------------|-----|
| Dependência do nome do host | 203 |
|---------------------------------------|-----|

| | |
|---|-----|
| Compreendendo os Resolvedores. | 203 |
| Compreendendo as Ordens de Procura das Informações de Configuração | 204 |
| Ordens de Procura Usadas no Ambiente do z/OS UNIX | 204 |
| Arquivos de Base da Configuração do Resolvedor | 205 |
| Tabelas de Conversão | 205 |
| Tabelas do Host Local | 206 |
| Aplicando Estas Informações de Configuração ao Developer for System z | 206 |
| O Endereço do Host Não É Resolvido Corretamente | 208 |

Bibliografia 211

| | |
|-------------------------------------|-----|
| Publicações Referenciadas | 211 |
| Publicações Informativas | 212 |

Glossário 215

Avisos 221

| | |
|---|-----|
| Licença de Copyright. | 224 |
| Reconhecimentos de Marca Registrada | 225 |

Índice. 227

Figuras

| | | | |
|--|----|--|-----|
| 1. Visão geral do componente. | 3 | 23. O número máximo de encadeamentos do conjunto de encadeamentos do RSE (mineradores de único encadeamento) | 92 |
| 2. RSE como um aplicativo Java | 5 | 24. Número máximo de encadeamentos do conjunto de encadeamentos do RSE (mineradores multiencadeados) | 92 |
| 3. donos das tarefas | 7 | 25. Número máximo de encadeamentos do JES Job Monitor. | 92 |
| 4. Fluxo de conexão | 8 | 26. Número máximo de encadeamentos do Debug Manager | 92 |
| 5. Depurador Integrado | 10 | 27. Uso de recursos com 5 logons | 96 |
| 6. Fluxo do CARMA | 11 | 28. Uso de recursos com 5 logons (continuação) | 96 |
| 7. Fluxo de Determinação de Enfileiramento de Conjunto de Dados | 13 | 29. Uso de recursos ao editar um membro PDS | 97 |
| 8. Estrutura de diretório do z/OS UNIX. | 15 | 30. Uso do espaço do sistema de arquivos z/OS UNIX | 99 |
| 9. Política AT-TLS para Debug Manager | 31 | 31. Uso do recurso de configuração de amostra | 112 |
| 10. Portas TCP/IP | 61 | 32. Definição de esquema LDAP de amostra | 128 |
| 11. update.sh - Suportar Configuração de DDVIPA com um Firewall. | 68 | 33. ADNJSAPAU - Administrative utility do CICSTS | 142 |
| 12. Amostra do Distributed Dynamic VIPA | 69 | 34. ADNJSAPAU - Utilitário Administrativo CICSTS (Parte 2 de 3). | 143 |
| 13. classificação WLM | 71 | 35. ADNJSAPAU - Utilitário Administrativo CICSTS (Parte 3 de 3). | 144 |
| 14. Número máximo de espaços de endereço | 82 | 36. RSEDSSL - Tarefa do usuário do daemon RSE para SSL | 188 |
| 15. Número de espaços de endereços por cliente | 83 | 37. Diálogo Importar Certificado do Host | 189 |
| 16. Número máximo de processos | 84 | 38. Diálogo Preferências - SSL | 190 |
| 17. Número de processos para STCRSE | 85 | | |
| 18. Número de processos por cliente | 85 | | |
| 19. O número máximo de encadeamentos do conjunto de encadeamentos do RSE (mineradores de único encadeamento) | 88 | | |
| 20. Número máximo de encadeamentos do conjunto de encadeamentos do RSE (mineradores multiencadeados) | 88 | | |
| 21. Número máximo de encadeamentos do JES Job Monitor. | 88 | | |
| 22. Número máximo de encadeamentos do Debug Manager | 88 | | |

Tabelas

| | | | |
|--|----|--|-----|
| 1. Comandos do Console do JES Job Monitor | 26 | 25. Contagem do espaço de endereço | 81 |
| 2. Matriz de Permissão do Comando LIMIT_COMMANDS | 27 | 26. Limites de espaço de endereço | 83 |
| 3. Perfis JESSPOOL Estendidos | 27 | 27. Contagem de processos | 83 |
| 4. Matriz de Autoridade do Console LIMIT_CONSOLE | 28 | 28. Limites do processo | 86 |
| 5. Matriz de permissão de navegação LIMIT_VIEW | 29 | 29. Contagem de encadeamentos | 86 |
| 6. Mecanismos de armazenamento de certificado SSL | 29 | 30. Limites de encadeamento | 89 |
| 7. Informações de SAF para Alterar Funções de Cliente | 35 | 31. Contagem de encadeamentos | 90 |
| 8. Informações do SAF de Push-to-client | 36 | 32. Limites de encadeamento | 93 |
| 9. Permissões relacionadas ao UNIXPRIV z/OS UNIX | 39 | 33. Configurações de Referência para Uso de Armazenamento | 95 |
| 10. Informações de SAF para Funções de Depuração | 40 | 34. Diretivas de saída do log | 99 |
| 11. Variáveis de configuração de segurança | 45 | 35. Diretivas de saída temporárias | 100 |
| 12. Comandos do Operador do JES2 Job Monitor | 53 | 36. Matriz de suporte ao grupo push-to-client para *.enabled | 123 |
| 13. Comandos do Operador do JES3 Job Monitor | 53 | 37. Matriz de suporte ao grupo push-to-client para reject.*.updates | 123 |
| 14. Subsistemas de Ponto de Entrada do WLM | 72 | 38. Concatenações de Grupo Push-to-client | 124 |
| 15. qualificadores de trabalho WLM | 72 | 39. Ligações do grupo de configuração da área de trabalho | 125 |
| 16. cargas de trabalho WLM | 73 | 40. Ligações do grupo do produto da área de trabalho | 125 |
| 17. cargas de trabalho WLM STC | 75 | 41. Informações do LDAP de Push-to-client | 127 |
| 18. Cargas de trabalho WLM OMVS | 75 | 42. Informações do SAF de Push-to-client | 132 |
| 19. Carga de trabalhos WLM JES | 76 | 43. Variáveis de JAVA_DUMP_TDUMP_PATTERN | 171 |
| 20. Cargas de trabalho WLM ASCH | 77 | 44. Mecanismos de armazenamento de certificado SSL | 184 |
| 21. Cargas de trabalho WLM - CICS | 77 | 45. Definições locais disponíveis para o resolver | 208 |
| 22. Uso de recursos comuns | 80 | 46. Publicações Referenciadas | 211 |
| 23. Uso de recursos obrigatórios específicos do usuário | 80 | 47. Web Sites Referidos | 212 |
| 24. Uso de recursos específicos do usuário | 80 | 48. Publicações Informativas | 212 |

Sobre este Documento

Este documento oferece informações de segundo plano para várias tarefas de configuração do próprio IBM® Rational Developer for System z e outros componentes e produtos do z/OS (como WLM e CICS).

De agora em diante, os seguintes nomes serão usados neste manual:

- *IBM Rational Developer for System z* é chamado *Developer for System z*.
- *IBM Rational Developer for System z Integrated Debugger* é chamado *Integrated Debugger*.
- *Common Access Repository Manager* é abreviado para *CARMA*.
- *Software Configuration and Library Manager Developer Toolkit* é chamado *SCLM Developer Toolkit*, abreviado como *SCLMDT*.
- O *z/OS UNIX System Services* é chamado de *z/OS UNIX*.
- O *Customer Information Control System Transaction Server* é chamado de *CICSTS*, abreviado para *CICS*.

Este documento faz parte de um conjunto de documentos que descrevem a configuração do host do Developer for System z. Cada um desses documentos tem um público alvo específico. Você não precisa ler todos os documentos para concluir a configuração do Developer for System z.

- *O Guia de Configuração de Host do IBM Rational Developer for System z* (S517-9094) descreve em detalhes todas as tarefas de planejamento, tarefas de configuração e opções (incluindo opcionais) e fornece cenários alternativos.
- *IBM Rational Developer for System z: Referência de Configuração de Host* (S517-9857) descreve o design do Developer for System z e oferece informações complementares para várias tarefas de configuração dos componentes do Developer for System z, z/OS e outros produtos (como WLM e CICS) relacionados ao Developer for System z.
- *Guia de Iniciação Rápida de Configuração de Host do IBM Rational Developer for System z* (G517-9391) descreve uma configuração mínima do Developer for System z.
- *IBM Rational Developer for System z Host Configuration Utility* (SC14-7282) descreve o Host Configuration Utility, um aplicativo de painel ISPF que orienta nas etapas de customização opcional básicas e comuns para o Developer for System z.

As informações neste documento aplicam-se a todos os pacotes IBM Rational Developer for System z Versão 9.1.1.

Para obter as versões mais atualizadas deste documento, consulte o Guia de Referência de Configuração de Host (SC14-7290) do *IBM Rational Developer for System z* disponível em <http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss?CTY=US&FNC=SRX&PBL=SC14-7290>.

Para obter as versões mais atualizadas da documentação completa, incluindo instruções de instalação, White Papers, podcasts e tutoriais, consulte a página de biblioteca do do website IBM Rational Developer for System z (http://www-01.ibm.com/software/sw-library/en_US/products/Z964267S85716U24/).

Quem Deve Usar este Documento

Este documento destina-se à configuração e ajuste dos programadores de sistema do IBM Rational Developer for System z Versão 9.1.1.

Enquanto as etapas de configuração reais são descritas em outra publicação, esta publicação lista em detalhes vários assuntos relacionados, como ajuste, configuração de segurança, entre outros. Para usar este documento, você deve estar familiarizado com os sistemas host z/OS UNIX System Services e MVS.

Resumo das Mudanças

Esta seção resume as mudanças para a Referência de Configuração de Host do *IBM Rational Developer for System z Versão 9.1.1*, SC43-1628-08 (atualização dezembro de 2014).

Mudanças técnicas e adições ao texto e ilustrações são indicadas por uma linha vertical à esquerda da mudança.

Novas informações:

- Perfis de Segurança Atualizados do Depurador Integrado. Consulte o “Segurança de Depuração” na página 40.
- Informações incluídas no Suporte ao Passphrase. Consulte o “Métodos de autenticação” na página 20.

Este documento contém informações anteriormente apresentadas na Referência de Configuração de Host do *IBM Rational Developer for System z Versão 9.1.1*, SC14-7290-07.

Novas informações:

- Informações incluídas sobre a segurança do arquivo de log. Consulte o “Segurança do arquivo de log” na página 37.
- Informações incluídas sobre o suporte ao grupo para rejeitar atualizações distribuir-para-cliente. Consulte o “Diversos Grupos de Desenvolvedores” na página 123.
- Informações sobre o uso de recurso atualizado. Consulte o Capítulo 5, “Considerações de Ajuste”, na página 79.
- Arquivo de log atualizado e informações de rastreamento. Consulte o Capítulo 12, “Resolução de problemas de configuração”, na página 163.

Esse documento contém informações apresentadas anteriormente na Referência de Configuração de Host do *IBM Rational Developer for System z Versão 9.0.1*, SC14-7290-06.

Novas informações:

- Informações incluídas na configuração do AT-TLS. Consulte o Capítulo 14, “Configurando o AT-TLS”, na página 195.

Esse documento contém informações apresentadas anteriormente na Referência de Configuração de Host do *IBM Rational Developer for System z Versão 9.0.1*, SC14-7290-05.

Novas informações:

- Informações incluídas sobre os nomes de arquivos de log com registro de data e hora. Consulte o “Arquivos de Log” na página 164.
- Informações incluídas sobre novos eventos auditáveis. Consulte Dados de auditoria.

Este documento contém informações anteriormente apresentadas na Versão 9.0 do *IBM Rational Developer for System zHost Configuration Reference*, SC14-7290-04.

Novas informações:

- Uso da porta atualizada do TCP/IP. Consulte o “Portas TCP/IP” na página 61.
- Incluída amostra para sincronizar automaticamente os dois daemons RSE. Consulte o “Sincronização Automatizada” na página 159.
- Informações incluídas sobre os novos arquivos de log. Consulte o “Arquivos de Log” na página 164.

Este documento contém informações apresentadas anteriormente no *IBM Rational Developer for System z Versão 8.5.1: Referência de Configuração de Host*, S517-9857-03.

Novas informações:

- Informações incluídas sobre perfis SAF para alterar funções de cliente. Consulte o “Alterando Funções de Cliente” na página 35.
- Números de uso do recurso atualizados. Consulte Capítulo 5, “Considerações de Ajuste”, na página 79
- Valor padrão atualizado para número máximo de usuários por conjunto de encadeamentos. Consulte o Capítulo 5, “Considerações de Ajuste”, na página 79.

Este documento contém informações anteriormente presentes na Referência de Configuração de Host do *IBM Rational Developer for System z Versão 8.5*, S517-9857-02.

Novas informações:

- Informações atualizadas de segurança do JES Job Monitor. Consulte o Capítulo 2, “Considerações de segurança”, na página 19.
- Informações incluídas sobre saídas de usuário. Consulte o Capítulo 9, “Considerações da Saída de Usuário”, na página 149.

Este documento contém informações apresentadas anteriormente no *IBM Rational Developer for System z Versão 8.0.3: Referência de Configuração de Host*, S517-9857-01.

Novas informações:

- Estrutura de diretório z/OS UNIX atualizada. Consulte o “Estrutura de diretório do z/OS UNIX” na página 15.
- Informações incluídas sobre controle de cliente baseado em host. Consulte o Capítulo 7, “Considerações de Push-to-client”, na página 119.
- Informações direcionar ao cliente relacionadas à segurança incluídas. Consulte o “Grupos de Desenvolvedores de Push-to-client” na página 36.
- Uso do documento de ACEEs Gerenciados. Consulte o “ACEE Gerenciado” na página 41.
- Informações incluídas sobre processamento de log de auditoria automatizado. Consulte o “Processamento de Auditoria” na página 25.
- Informações atualizadas sobre diretivas relacionadas a segurança e auditoria em arquivos de configuração. Consulte o “arquivos de configuração do Developer for System z” na página 42.

- Informações TCP/IP adicionais incluídas. Consulte o Capítulo 3, “Considerações de TCP/IP”, na página 61.
- Informações atualizadas de Autoridade de Certificação para comunicação SSL. Consulte o Capítulo 13, “Configurando o SSL e a Autenticação X.509”, na página 183.
- Uso do recurso atualizado. Consulte o “Uso de Recursos” na página 79.

Este documento contém informações apresentadas anteriormente no *IBM Rational Developer for System z Versão 8.0.1 Referência de Configuração de Host*, S517-9857-00.

Novas informações:

- Seção CARMA em Entendendo o Developer for System z. Consulte “CARMA” na página 10.
- Informações gerais relacionadas ao TCP/IP. Consulte o Capítulo 3, “Considerações de TCP/IP”, na página 61.
- Resolução do encerramento anormal por falta de espaço B37. Consulte o “Encerramento Anormal por Falta de Espaço B37 de Feedback de Erro” na página 180.

Informações removidas:

- As informações apresentadas anteriormente no Guia de Configuração de Host do *IBM Rational Developer para System z Versão 7.6.1* (SC23-7658-04) agora são divididas em dois documentos: Guia de Configuração de Host *IBM Rational Developer for System z* (SC23-7658) e Referência de Configuração do Host do *IBM Rational Developer for System z* (SC14-7290).
- As informações referentes à configuração do APPC foram movidas para o White Paper *Using APPC to provide TSO command services* (SC14-7291).
- Configurando o INETD

Descrição do Conteúdo do Documento

Esta seção resume as informações apresentadas neste documento.

Entendendo o Developer for System z

O host do Developer for System z consiste em vários componentes que interagem para oferecer acesso ao cliente para os serviços e dados do host. Entender o design desses componentes pode ajudá-lo a tomar as decisões corretas de configuração.

Considerações de segurança

O Developer for System z fornece acesso ao mainframe para usuários de uma estação de trabalho sem mainframe. A validação dos pedidos de conexão, o fornecimento de comunicação segura entre o host e a estação de trabalho, e a atividade de autorização e auditoria são aspectos importantes da configuração do produto.

Considerações de TCP/IP

O Developer for System z usa TCP/IP para fornecer acesso ao mainframe para usuários de uma estação de trabalho sem mainframe. Ele também usa TCP/IP para comunicação entre vários componentes e outros produtos.

Considerações WLM

Ao contrário dos aplicativos tradicionais do z/OS, o Developer for System z não é um aplicativo monolítico que pode ser identificado facilmente para Workload Manager (WLM). O Developer for System z consiste de vários componentes que interagem para fornecer ao cliente acesso para os serviços e dados do host. Alguns destes serviços estão ativos em diferentes espaços de endereço, resultando em diferentes classificações de WLM.

Considerações de Ajuste

O RSE (Explorador de Sistema Remoto) é o núcleo do Developer for System z. Para gerenciar as conexões e as cargas de trabalho a partir dos clientes, o RSE é formado por um espaço de endereço do daemon, que controla os espaços de endereços do conjunto de encadeamento. O daemon age como um ponto focal para fins de conexão e gerenciamento, enquanto os conjuntos de encadeamentos processam as cargas de trabalho do cliente.

Isso torna o RSE um alvo principal para o ajuste da configuração do Developer for System z. Entretanto, a manutenção de centenas de usuários, cada um usando 17 ou mais encadeamentos, uma determinada quantidade de armazenamento e possivelmente um ou mais espaços de endereço exige configuração adequada do Developer for System z e do z/OS.

Considerações sobre Desempenho

O z/OS é um sistema operacional altamente customizável, e (algumas vezes pequenas) alterações no sistema podem ter um grande impacto sobre o desempenho geral. Este capítulo destaca algumas das alterações que podem ser feitas para melhorar o desempenho do Developer for System z.

Considerações de Push-to-client

Push-to-client, ou controle de cliente baseado em host, suporta gerenciamento central dos seguintes itens:

- Arquivos de configuração do cliente
- Versão de produto do cliente
- Definições de projeto

considerações CICSTS

Este capítulo contém informações úteis para um administrador do CICS Transaction Server.

Considerações da Saída de Usuário

Esse capítulo o ajuda a aprimorar o Developer for System z ao gravar as rotinas de saída.

Customizando o Ambiente TSO

Este capítulo ajuda você a imitar um procedimento de logon do TSO incluindo instruções DD e conjuntos de dados no ambiente do TSO no Developer for System z.

Executando várias instâncias

Há situações em que você deseja várias instâncias do Developer for System z ativas no mesmo sistema, por exemplo, durante o teste de um upgrade. Entretanto,

alguns recursos, como portas TCP/IP, não podem ser compartilhadas, portanto os padrões nem sempre são aplicáveis. Use as informações neste capítulo para planejar a coexistência de diferentes instâncias do Developer for System z; depois é possível usar este guia de configurações para customizá-las.

Resolução de problemas de configuração

Este capítulo é fornecido para ajudá-lo com alguns problemas comuns que você pode encontrar durante a configuração do seu Developer for System z, e possui as seções a seguir:

- Análise de Log e Configuração Usando FEKLOGS
- Arquivos de Log
- Arquivos de dump
- Rastreio
- Bits de permissão do z/OS UNIX
- Portas TCP/IP reservadas
- Tamanho do espaço de endereço
- Transação APPC e serviço TSO Commands
- Informações Variadas

Configurando o SSL e a Autenticação X.509

Essa seção é fornecida para ajudá-lo com alguns problemas comuns que podem ser encontrados durante a configuração da Secure Socket Layer (SSL) ou durante a verificação ou modificação de uma configuração existente. Essa seção também fornece uma configuração de amostra para suportar que os usuários se autenticuem com um certificado X.509.

Configurando o TCP/IP

Essa seção é fornecida para ajudá-lo com alguns problemas comuns que podem ser encontrados durante a configuração do TCP/IP ou durante a verificação ou modificação de uma instalação existente.

Guia de Referência de Configuração do Host do IBM Rational Developer for System z

Capítulo 1. Entendendo o Developer for System z

O host do Developer for System z consiste em diversos componentes que interagem para dar ao cliente acesso aos dados e serviços do host. Entender o design desses componentes pode ajudá-lo a tomar as decisões corretas de configuração.

Os seguintes tópicos são abordados neste capítulo:

- “Visão geral do componente”
- “RSE como um aplicativo Java” na página 5
- “donos das tarefas” na página 6
- “Fluxo de conexão” na página 8
- “Depurador Integrado” na página 10
- “CARMA” na página 10
- “Proprietário de Bloco de Conjunto de Dados” na página 13
- “Estrutura de diretório do z/OS UNIX” na página 15

Visão geral do componente

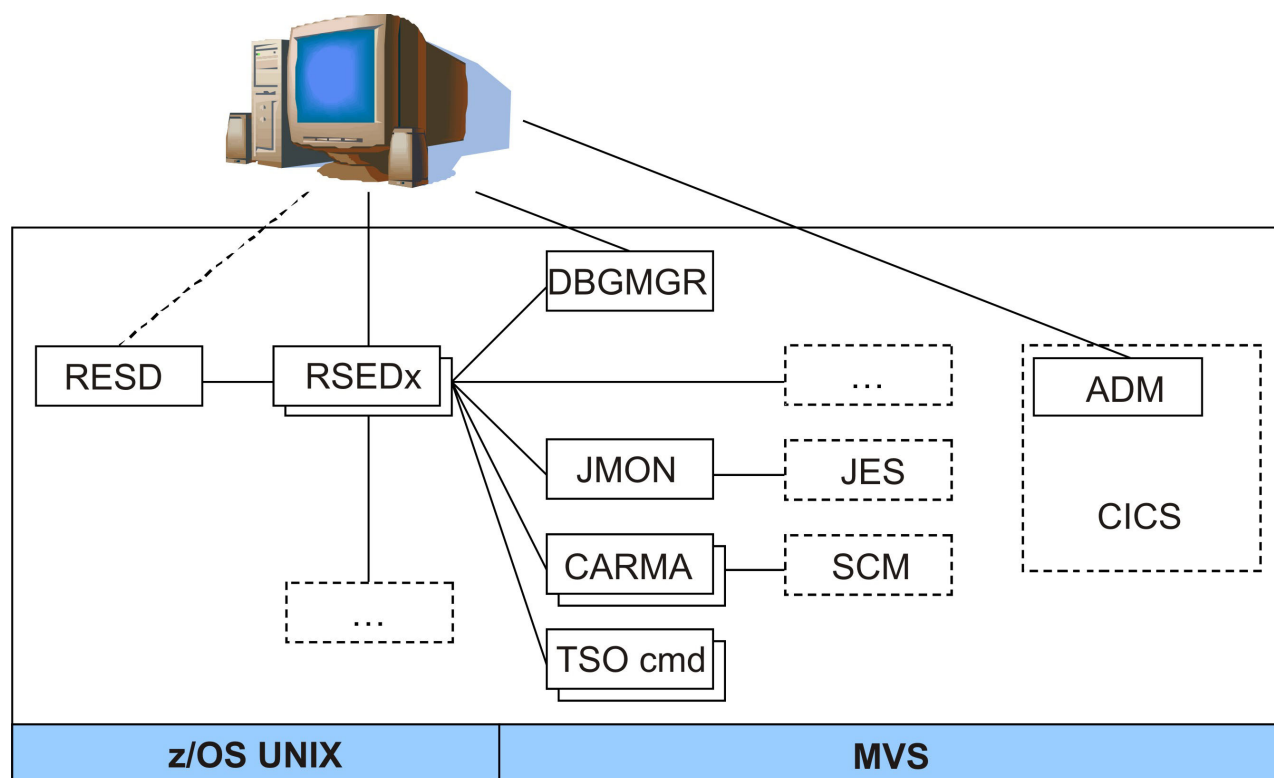


Figura 1. Visão geral do componente

Figura 1 mostra uma visão geral do layout do Developer for System z em seu sistema host.

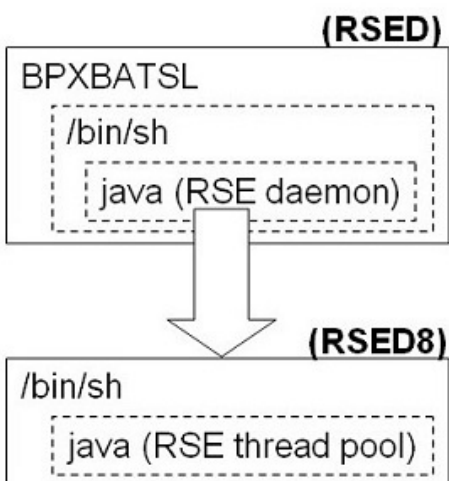
- O Remote Systems Explorer (RSE) fornece os serviços principais, como conectar o cliente ao host e iniciar outros servidores para serviços específicos. O RSE consiste em duas entidades lógicas:
 - O daemon RSE (RSED), que gerencia a configuração de conexão. O daemon RSE também é responsável pela execução em modo de servidor único. Para fazer isso, o daemon RSE cria um ou mais processos-filho conhecidos como conjuntos de encadeamento do RSE (RSEDx).
 - Servidor RSE, que manipula pedidos individuais do cliente. Um servidor RSE é ativado como um encadeamento dentro de um conjunto de encadeamento do RSE.
- O Gerenciador de Depuração (DBGMR) coordena a atividade do Depurador Integrado.
- O Serviço TSO Commands (TSO cmd) fornece uma interface como um lote para os comandos TSO e ISPF.
- O JES Job Monitor (JMON) fornece todos os serviços relacionados ao JES.
- O Common Access Repository Manager (CARMA) fornece uma interface para interagir com Software Configuration Managers (SCMs), como o CA Endevor.
- O SCLM Developer Toolkit (SCLMDT) fornece uma interface para aprimorar e interagir com SCLM.
- O Application Deployment Manager (ADM) fornece vários serviços relacionados ao CICS.
- Mais serviços estão disponíveis, que podem ser fornecidos pelo próprio Developer for System z ou o software de correquisito.

A descrição no parágrafo e a lista mostram a função central designada ao RSE. Com algumas exceções, toda a comunicação do cliente passa pelo RSE. Isso é permitido para uma configuração fácil da rede relacionada à segurança, uma vez que apenas um conjunto limitado de portas é usado para a comunicação entre o cliente e o host.

Para gerenciar as conexões e as cargas de trabalho a partir dos clientes, o RSE é formado por um espaço de endereço do daemon, que controla os espaços de endereços do conjunto de encadeamento. O daemon age como um ponto focal para fins de conexão e gerenciamento, enquanto os conjuntos de encadeamentos processam as cargas de trabalho do cliente. Com base nos valores definidos no arquivo de configuração `rsed.envvars` e na quantidade real de conexões do cliente, vários espaços de endereço do conjunto de encadeamento podem ser iniciados pelo daemon.

RSE como um aplicativo Java

z/OS UNIX processes



Java storage usage

| |
|-----------------------------|
| System - shared |
| System - private |
| Code (z/OS UNIX, Java, RSE) |
| Java heap |
| Not in use |

| JOBNAME | Status | PID | PPID | Command |
|---------|----------------------|----------|----------|-------------|
| RSED | FILE SYS KERNEL WAIT | 50331904 | 1 | BPXBATSL |
| RSED | WAITING FOR CHILD | 67109114 | 50331904 | /bin/sh ... |
| RSED | FILE SYS KERNEL WAIT | 50331949 | 67109114 | java ... |
| RSED8 | WAITING FOR CHILD | 307 | 50331949 | /bin/sh ... |
| RSED8 | FILE SYS KERNEL WAIT | 308 | 307 | java ... |

Figura 2. RSE como um aplicativo Java

A Figura 2 mostra uma visualização básica do uso de recursos (processos e armazenamento) pelo RSE.

O RSE é um aplicativo Java[™], que significa que ele está ativo no ambiente z/OS UNIX. Isso é permitido para facilitar o porting em diferentes plataformas host e comunicação direta com o cliente do Developer for System z, que é também um aplicativo Java (baseado na estrutura do Eclipse). Portanto, o conhecimento básico de como z/OS UNIX e Java funcionam é muito útil quando você tenta compreender o Developer for System z.

No z/OS UNIX, um programa é executada em um processo, que é identificado por um PID (ID do Processo). Cada programa é ativado em seu próprio processo, portanto invocar outro programa criará um novo processo. O processo que iniciou um processo é referenciado com um PPID (PID Pai), o novo processo é chamado de processo-filho. O processo-filho pode ser executado no mesmo espaço de endereço ou pode ser gerado (criado) em um novo espaço de endereço. Um novo processo que é executado no mesmo espaço de endereço pode ser comparado a executar um comando em TSO, enquanto aquele gerado em um novo espaço de endereço é semelhante a enviar uma tarefa em lote.

Observe que um processo pode ser único ou multiencadeado. Em um aplicativo multiencadeado (como o RSE), os diferentes encadeamentos competem por recursos do sistema como se eles fossem espaços de endereço separados (com menos gasto adicional).

Mapeando essas informações de processo para a amostra RSE na Figura 2 na página 5, obtivemos o seguinte fluxo:

1. Quando a tarefa RSED for iniciada, ela executa BPXBATSL, que invoca z/OS UNIX e cria um ambiente de shell – PID 50331904.
2. Neste processo, o shell script rsed.sh é executado, que executa em um processo separado (/bin/sh) – PID 67109114.
3. O shell script configura as variáveis de ambiente definidas em rsed.envvars e executa o Java com os parâmetros necessários para iniciar o daemon RSE – PID 50331949.
4. O daemon RSE fará spawn off do novo shell em um processo-filho (RSED8) – PID 307.
5. Neste shell, as variáveis de ambiente definidas em rsed.envvars são configuradas e o Java é executado com os parâmetros necessários para iniciar o conjunto de encadeamento do RSE – PID 308.

O RSE é capaz de executar em modo de endereçamento de 31 bits ou 64 bits, resultando em diferentes limites de armazenamento. No modo de 31 bits, o armazenamento disponível está limitado a 2 GB, enquanto que no modo de 64 bits, não há limite, a menos que especificado no SYS1.PARMLIB.

Aplicativos Java, como o RSE, não alocam armazenamento diretamente, mas usam serviços de gerenciamento de memória Java. Esses serviços, como alocação de armazenamento, liberação de armazenamento e coleta de lixo, funcionam dentro dos limites do heap Java. Os tamanhos mínimo e máximo do heap é definido (implicitamente ou explicitamente) durante a inicialização de Java. Ao executar em modo de 64 bits, o Java tentará alocar o heap acima de 2 GB de barramento, liberando espaço abaixo do barramento.

Isso significa que a obtenção da maioria do tamanho de espaço de endereço disponível é um ato de equilíbrio da definição de um tamanho grande de heap, enquanto deixa espaço suficiente para o z/OS armazenar uma quantidade variável de blocos de controle do sistema (dependendo do número de encadeamentos ativos).

donos das tarefas

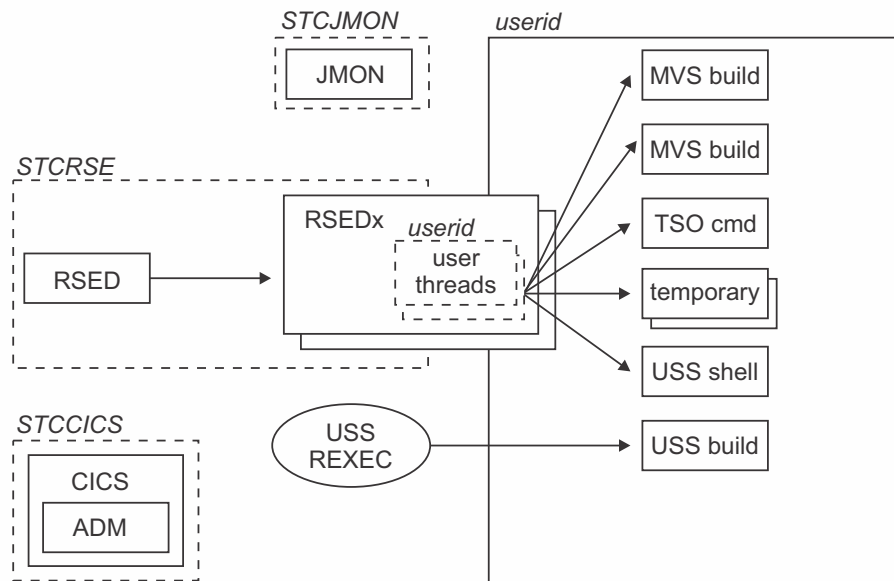


Figura 3. donos das tarefas

Figura 3 mostra uma visão geral básica do proprietário das credenciais de segurança usadas para várias tarefas do Developer for System z.

A propriedade de uma tarefa pode ser dividida em duas seções. As tarefas iniciadas são propriedades do ID do usuário que é designado para a tarefa iniciada em seu software de segurança. Todos as outras tarefas, com os conjuntos de encadeamentos (RSEDx) como exceção, são propriedades do ID de usuário cliente.

Figura 3 mostra as tarefas iniciadas do Developer for System z (DBGMGR, JMON e RSED), as tarefas iniciadas de amostra e os serviços de sistema com os quais o Developer for System z se comunica. O Application Deployment Manager (ADM) fica ativo dentro de uma região CICS. A tag USS REXEC representa o serviço do z/OS UNIX REXEC (ou SSH).

O daemon RSE (RSED) cria um ou mais espaços de endereço do conjunto de encadeamentos (RSEDx) para processar os pedidos dos clientes. Cada conjunto de encadeamentos RSE suporta múltiplos clientes e é propriedade do mesmo usuário como um daemon RSE. Cada cliente possui seus próprios encadeamentos dentro de um conjunto de encadeamentos, e estes encadeamentos são propriedades do ID de usuário cliente.

Dependendo das ações concluídas pelo cliente, um ou mais espaços de endereço adicionais podem ser iniciados, todos propriedades do ID de usuário cliente, para executar uma ação solicitada. Esses espaços de endereço podem ser uma tarefa em lote MVS, uma transação APPC ou um processo-filho z/OS UNIX. Observe que um processo-filho z/OS UNIX está ativo em um inicializador z/OS UNIX (BPXAS) e o processo-filho aparece com uma tarefa iniciada no JES.

A criação destes espaços de endereços é mais frequentemente acionada por um encadeamento do usuário em um conjunto de encadeamentos, diretamente ou usando serviços do sistema como ISPF. Mas o espaço de endereço também poderia ser criado por um terceiro. Por exemplo, z/OS UNIX REXEC ou SSH são envolvidos quando iniciam construções no z/OS UNIX.

Os espaços de endereços do usuário terminam com a conclusão da tarefa ou quando um cronômetro de inatividade vence. As tarefas iniciadas permanecem ativas. Os espaços de endereços listados em Figura 3 na página 7 permanecem no sistema tempo suficiente para serem visíveis. No entanto, é recomendável estar ciente que, devido à maneira com que o z/OS UNIX é projetado, há também vários espaços de endereço temporários de curta duração.

Fluxo de conexão

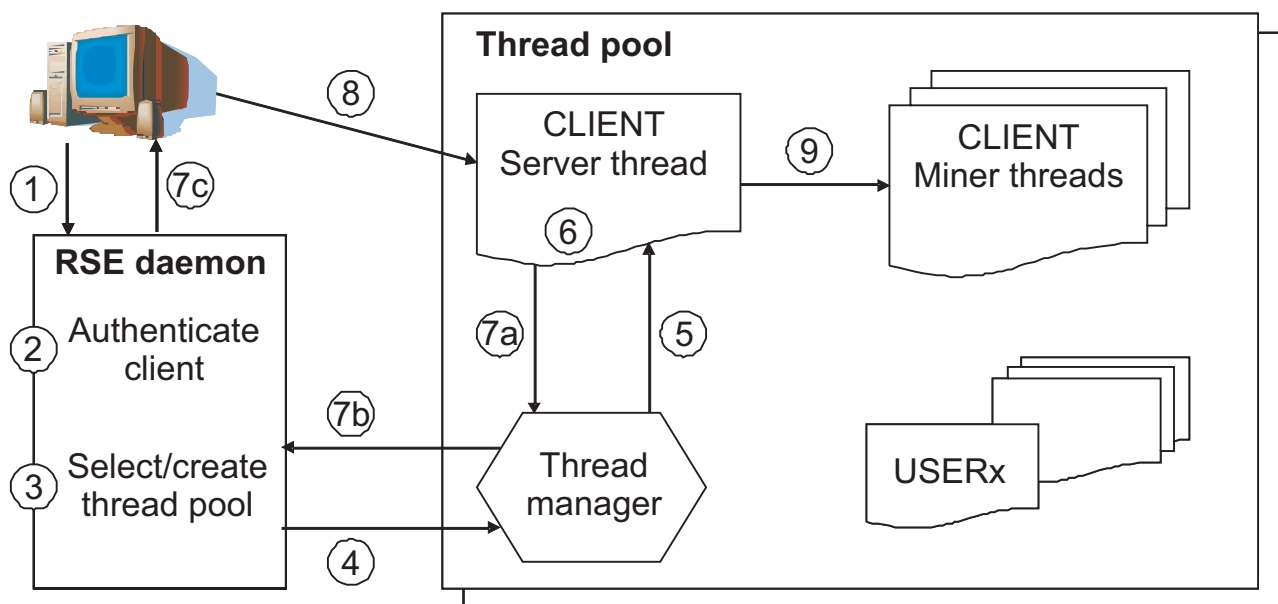


Figura 4. Fluxo de conexão

Figura 4 mostra uma visão geral esquemática de como o cliente conecta-se ao host usando Developer for System z. Ele também explica brevemente como os PassTickets são usados.

1. O cliente efetua login no daemon (porta 4035).
2. O daemon RSE autentica o cliente usando as credenciais apresentadas pelo cliente.
3. O daemon RSE seleciona um conjunto de encadeamento existente ou inicia um novo se todos estiverem cheios.
4. O daemon RSE passa o ID do usuário cliente para o conjunto de encadeamento.
5. O conjunto de encadeamento cria um encadeamento do servidor RSE específico do cliente, usando o ID do usuário cliente e um PassTicket para autenticação.
6. O encadeamento do servidor cliente se conecta a uma porta para comunicação futura com o cliente.
7. O encadeamento do servidor cliente retorna o número da porta à qual o cliente deve se conectar.

8. O cliente desconecta do daemon RSE e se conecta ao número da porta fornecido.
9. O encadeamento do servidor cliente inicia outros encadeamentos específicos do usuário (extratores), sempre usando o ID do usuário cliente e um PassTicket para autenticação. Esses encadeamentos fornecem os serviços específicos do usuário necessários pelo cliente.

A descrição anterior mostra o design orientado a encadeamento do RSE. Em vez de iniciar um espaço de endereço por usuário, vários usuários são atendidos por um espaço de endereço de um único conjunto de encadeamento. No conjunto de encadeamentos, cada extrator (um serviço específico do usuário) fica ativo em seu próprio encadeamento com o contexto de segurança do usuário designado a ele, garantindo uma configuração segura. Esse design acomoda um grande número de usuários com uso de recursos limitado, mas não significa que cada cliente usará vários encadeamentos (17 ou mais, dependendo das tarefas executadas).

Do ponto de vista da rede, o Developer para System z atua de forma semelhante ao FTP no modo passivo. O cliente se conecta a um ponto focal (daemon RSE) e, em seguida, elimina a conexão e reconecta ao número de porta fornecido pelo ponto focal. A seguinte lógica controla a seleção da porta que é usada na segunda conexão:

1. Se o cliente especificou um número de porta diferente de zero na guia de propriedades de subsistema, então o servidor RSE usará essa porta para a conexão. Se essa porta não estiver disponível, a conexão falhará.
2. Se `_RSE_PORTRANGE` for especificado em `rsed.envvars`, então o servidor RSE se conectará a uma porta desse intervalo. Se nenhuma porta estiver disponível, a conexão falhará. O servidor RSE não precisa da porta exclusivamente pela duração da conexão do cliente. Ela só é necessária no momento da expansão entre (servidor) a ligação e (cliente) a conexão que nenhum outro servidor RSE pode se conectar à porta. Isso significa que a maioria das conexões estará usando a primeira porta no intervalo, com o restante do intervalo sendo um buffer no caso de diversos logons simultâneos.
3. Se nenhuma limitação for configurada, o servidor RSE se conectará à porta 0. O resultado é que o TCP/IP escolhe o número da porta.

O uso de PassTickets para todos os serviços de z/OS que requerem autenticação permite que o Developer for System z chame esses serviços sem armazenar a senha ou avise constantemente o usuário para fazê-lo. O uso de PassTickets para todos os serviços z/OS permite também métodos de autenticação alternativos durante o login, como senhas únicas e certificados X.509.

Depurador Integrado

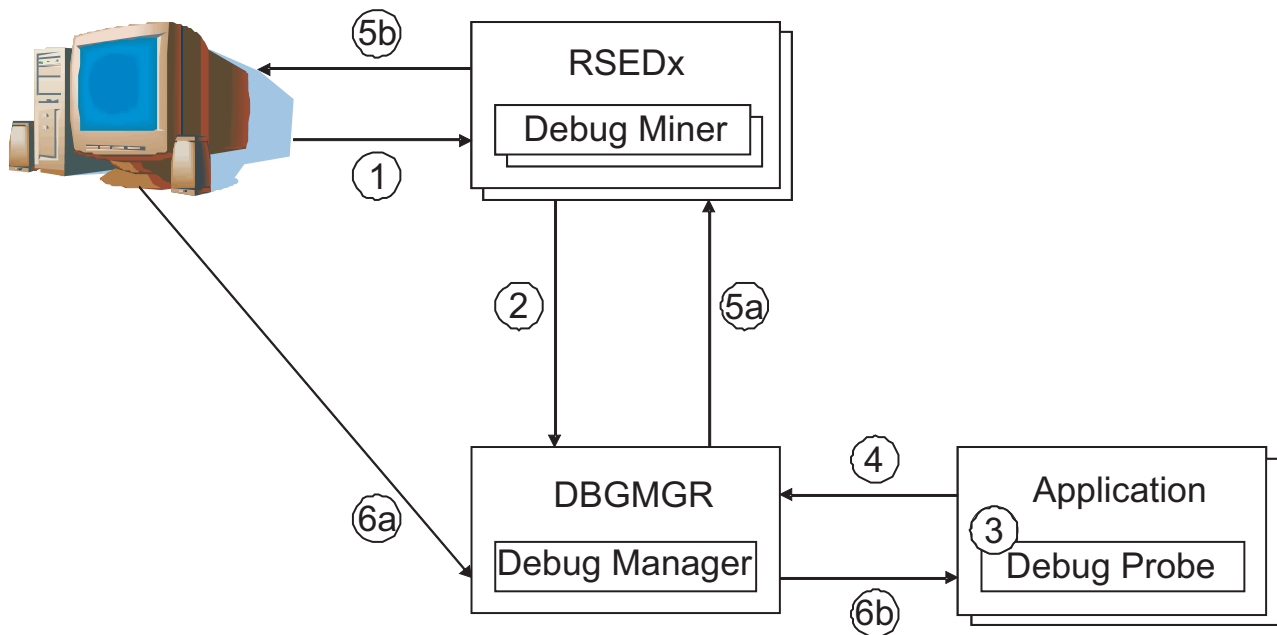


Figura 5. Depurador Integrado

O Depurador Integrado é usado para depurar vários aplicativos. A figura 5 mostra uma visão geral esquemática de como um cliente do Developer for System z pode depurar um aplicativo.

1. O cliente se conecta ao host, usando o logon do host do Developer for System z normal.
2. Como parte do logon, um extrator de depuração registrará o usuário com o gerenciador de depuração, o qual está ativo na tarefa iniciada de DBGMGR.
3. Quando um aplicativo for iniciado com um indicador de que ele deve ser depurado, o ambiente de linguagem (LE) chamará a análise de depuração.
4. A análise de depuração se registrará no gerenciador de depuração.
5. Usando o extrator de depuração, o gerenciador de depuração notificará o cliente do Developer for System z do usuário que receberá esta sessão de depuração. Se o usuário não estiver registrado neste momento, a sessão de depuração ficará inativa, esperando o usuário se registrar no gerenciador de depuração.
6. O mecanismo de depuração dentro do cliente contata o gerenciador de depuração, o qual por sua vez transmitirá os dados entre o mecanismo de depuração e a análise de depuração.

CARMA

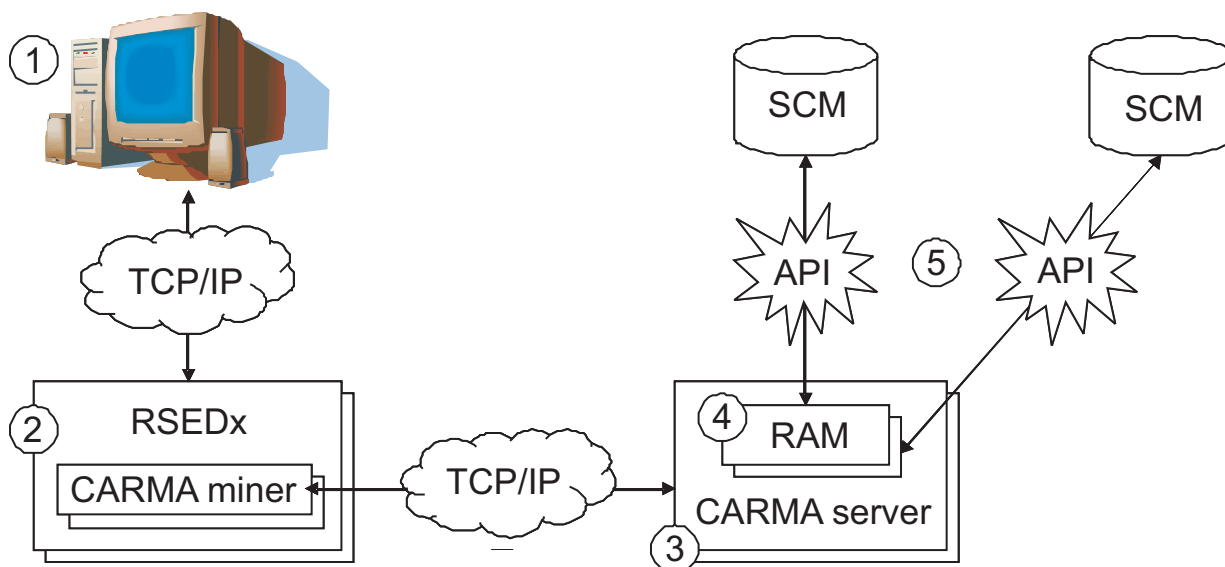


Figura 6. Fluxo do CARMA

O CARMA (Common Access Repository Manager) é usado para acessar um host baseado em Software Configuration Manager (SCM), por exemplo, o CA Endeavor® SCM. A Figura 6 mostra uma visão geral esquemática de como um cliente Developer for System z pode acessar qualquer Software Configuration Manager (SCM) baseado em host suportado.

1. O cliente tem um plug-in Common Access Repository Manager (CARMA).
2. O plug-in CARMA se comunica com o extrator CARMA, ativo como um encadeamento específico do usuário no conjunto de encadeamentos RSE (RSEDx). Esta comunicação é feita por meio da conexão RSE existente.
3. Quando o cliente solicitar acesso a um SCM, o extrator CARMA se conectará a uma porta TCP/IP e iniciará um servidor CARMA específico do usuário, com o número da porta como argumento de inicialização. O servidor CARMA então se conectará a esta porta e usará este caminho para se comunicar com o cliente. Note que o host baseado em SCMs espera espaços de endereço de usuário único para acessar os seus serviços, que requer que o CARMA inicie um servidor CARMA por usuário. Não é possível criar um único servidor que suporte diversos usuários.
4. O servidor CARMA carregará o Repository Access Manager (RAM) que suporta o SCM solicitado.
5. O RAM lida com os detalhes técnicos de interação com o SCM específico e apresenta uma interface comum para o cliente.

Arquivos de Configuração CARMA

O Developer for System z suporta vários métodos para iniciar um servidor CARMA. Cada método tem vantagens e desvantagens. O Developer for System z também fornece vários Repository Access Managers (RAMs), os quais podem ser divididos em dois grupos, RAMs de produção e RAMs de amostra. Várias combinações de RAMs e métodos de inicialização do servidor estão disponíveis como uma configuração pré-configurada.

Todos os métodos de inicialização do servidor compartilham um arquivo de configuração comum, CRASRV.properties, o qual (junto com outras coisas) especifica qual método de inicialização será usado.

CRASTART

O método "CRASTART" inicia o servidor CARMA como uma subtarefa dentro do RSE. Ele fornece uma configuração bastante flexível utilizando um arquivo de configuração separado, que define alocações de conjuntos de dados, e chamadas de programas necessárias para iniciar um servidor CARMA. Esse método fornece o melhor desempenho e utiliza o mínimo de recursos, mas requer que o módulo CRASTART esteja localizado no LPA.

O RSE chama o módulo de carregamento CRASTART, o qual usa as definições em crastart*.conf para criar um ambiente válido para executar comandos ISPF e TSO em lote. O Developer for System z usa este ambiente para executar o servidor CARMA, CRASERV. O Developer for System z fornece vários arquivos crastart*.conf, cada um deles pré-configurado para um RAM específico.

Envio em Lote

O método "envio em lote" inicia o servidor CARMA enviando uma tarefa. Esse é o método padrão utilizado nos arquivos de configuração de amostra fornecidos. O benefício desse método é que os logs do CARMA são facilmente acessados na saída de tarefas. Ele também permite o uso de JCL de servidor customizado para cada desenvolvedor, que é mantido pelo próprio desenvolvedor. Entretanto, esse método utiliza um iniciador de JES por desenvolvedor que inicia um servidor CARMA.

O RSE chama o CLIST CRASUB*, o qual por sua vez envia um JCL embutido para criar um ambiente válido para executar os comandos ISPF e TSO em lote. O Developer for System z usa este ambiente para executar o servidor CARMA, CRASERV. O Developer for System z fornece vários membros CRASUB*, cada um deles pré-configurado para um RAM específico.

Proprietário de Bloco de Conjunto de Dados

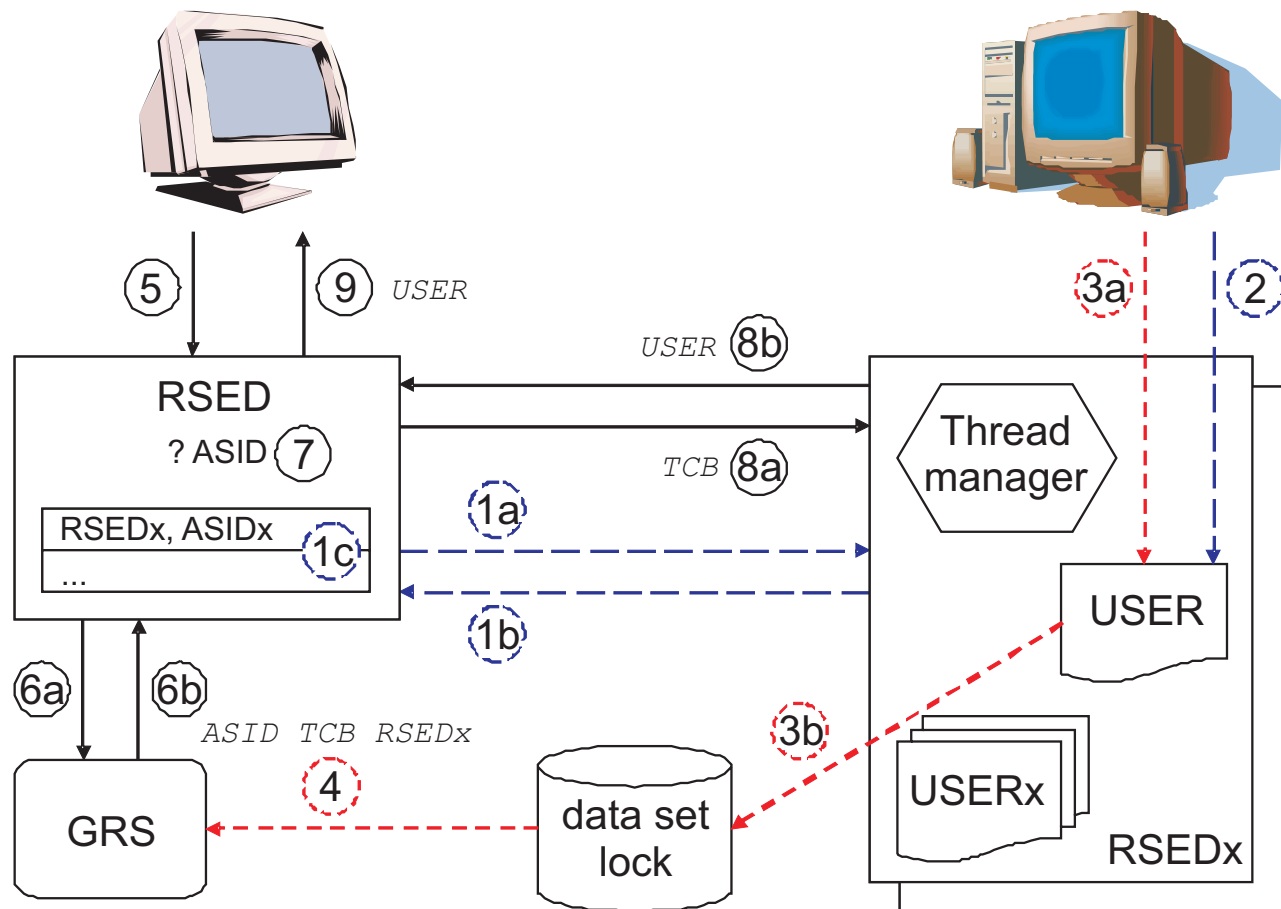


Figura 7. Fluxo de Determinação de Enfileiramento de Conjunto de Dados

Figura 7 mostra uma visão geral esquemática de como o daemon RSE determina qual cliente Developer for System z possui um bloqueio de conjunto de dados.

1. RSE daemon (RSED) cria um conjunto de encadeamentos (RSEDx). Para confirmar a conclusão da inicialização, o conjunto de encadeamentos relata seu Address Space Identifier (ASID) novamente ao daemon RSE, que armazena-o no bloco de controle criado para rastrear este conjunto de encadeamento.
2. O cliente efetua login, que cria um encadeamento do servidor RSE específico do usuário (USER) dentro de um conjunto de encadeamento (RSEDx). Cada encadeamento tem um identificador exclusivo de Task Control Block (TCB).
3. O cliente abre um conjunto de dados na edição, que instrui o servidor RSE a obter um bloqueio restrito (enfileiramento) no conjunto de dados.
4. O sistema registra o ASID, TCB e o nome da tarefa (RSEDx) do solicitante como parte do processo de enfileiramento. Essas informações são armazenadas nas filas GRS (Global Resource Serialization).
5. Um operador consulta o daemon RSE para o status do bloqueio do conjunto de dados.
6. O daemon RSE varre as filas GRS para saber se o conjunto de dados está bloqueado e recupera o ASID, TCB e o nome da tarefa do proprietário do bloqueio.

7. O ASID recuperado é comparado com o ASID dos conjuntos de encadeamentos diferentes.
8. O daemon RSE solicita que o conjunto de encadeamentos que possui o ASID determine qual usuário possui o TCB.
9. O ID do usuário do cliente relacionado é retornado ao solicitante quando uma correspondência for encontrada. Caso contrário, o nome da tarefa recuperado de GRS é retornado.

Com a configuração do servidor único do Developer for System z, em que diversos usuários são designados a um único espaço de endereço de encadeamento, o z/OS perdeu a capacidade de rastrear quem possui um bloqueio em um conjunto de dados ou membro com o comando do operador **DISPLAY GRS,RES=(*,dataset*)**. Os comandos do sistema param no nível de espaço de endereço, que é o conjunto de encadeamento.

Para abordar este problema, o Developer for System z fornece o comando do operador **MODIFY rsed APPL=DISPLAY OWNER,DATASET=dataset**, conforme descrito em "Comandos de operador" em *Guia de Configuração do Host* (S517-9094). O comando do operador pode resolver todos os conjuntos de dados e bloqueios de membro feitos por usuários RSE, bem como bloqueios feitos por outros produtos, como ISPF.

Liberando um Bloqueio

Sob circunstâncias normais, um conjunto de dados ou um membro fica bloqueado quando o cliente o abre no modo de edição, e liberado quando o cliente fechar a sessão de edição.

Determinadas condições de erro podem evitar que esse mecanismo funcione como designado. Nesse caso, o usuário que mantém o bloqueio pode ser cancelado usando o comando do operador **modify cancel** do RSE, como descrito em "Comandos do operador" no *Guia de Configuração do Host* (SC23-7658). Os bloqueios do conjunto de dados ativo que pertencem a esse usuário são liberados durante o processo.

Estrutura de diretório do z/OS UNIX

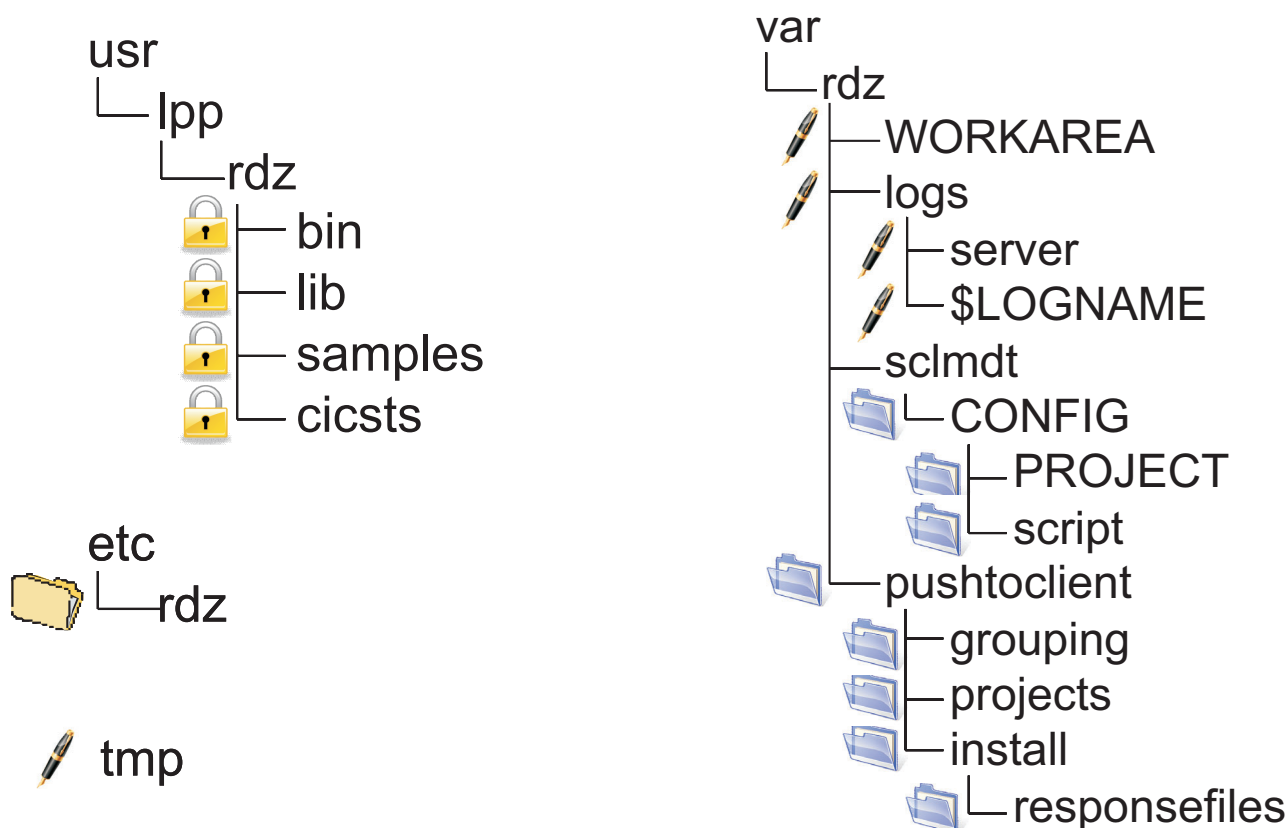


Figura 8. Estrutura de diretório do z/OS UNIX

Figura 8 mostra uma visão geral dos diretórios do z/OS UNIX usados pelo Developer for System z. A lista a seguir descreve cada diretório tocado pelo Developer for System z, como o local pode ser alterado e que mantém os dados dentro dele.

- `/usr/lpp/rdz/` é o caminho raiz para o código do produto do Developer for System z. O local real é especificado na tarefa iniciada RSED (variável HOME). Os arquivos contidos serão mantidos por SMP/E.
- `/etc/rdz/` contém o RSE e os arquivos de configuração relacionados ao extrator. O local real é especificado na tarefa iniciada RSED (variável CNFG). Os arquivos contidos são mantidos pelo programador de sistema.
- `/tmp/` é usado pelo TSO/ISPF Client Gateway do ISPF e vários extratores para armazenar dados temporários. Alguns IVPs armazenam sua saída aqui. Os arquivos contidos são mantidos pelo ISPF, pelos extratores e pelos IVPs. O local pode ser customizado com a variável TMPDIR no `rsed.envvars`. É também o local padrão para arquivos dump Java, que podem ser customizados com a variável `_CEE_DUMPTARG` em `rsed.envvars`.

Nota: `/tmp/` exige a máscara de bit de permissão 777 para permitir que cada cliente crie arquivos temporários.

- `/var/rdz/WORKAREA/` é usado pelo TSO/ISPF Client Gateway e SCLMDT do ISPF para transferir dados entre o z/OS UNIX e os espaços de endereço baseados em MVS. O local real é especificado em `rsed.envvars` (variável CGI_ISPWORK). Os arquivos contidos são mantidos pelo ISPF e SCLMDT.

Nota: /var/rdz/WORKAREA/ exige a máscara de bit de permissão 777 para permitir que cada cliente crie arquivos temporários.

- /var/rdz/logs/server/ mantém os logs do daemon RSE e dos servidores do conjunto de encadeamento do RSE. O local real é especificado em rsed.envvars (variável daemon.log). Os arquivos contidos são mantidos por RSE.
- /var/rdz/logs/\$LOGNAME/ mantém os logs específicos do usuário dos extratores e do servidor RSE. O local real é especificado em rsed.envvars (variáveis user.log e DSTORE_LOG_DIRECTORY). Os arquivos contidos são mantidos pelo RSE e pelos extratores.

Nota: /var/rdz/logs/ exige a máscara de bit de permissão 777 para permitir que cada cliente crie seu diretório \$LOGNAME e armazene os arquivos de log específicos do usuário.

- /var/rdz/sclmdt/CONFIG/ mantém os arquivos de configuração gerais do SCLMDT. O local real é especificado em rsed.envvars (variável SCLMDT_CONF_HOME). Os arquivos contidos são mantidos pelo administrador do SCLM.
- /var/rdz/sclmdt/CONFIG/PROJECT/ mantém os arquivos de configuração do projeto SCLMDT. O local real é especificado em rsed.envvars (variável SCLMDT_CONF_HOME). Os arquivos contidos são mantidos pelo administrador do SCLM.
- /var/rdz/sclmdt/CONFIG/script/ mantém os scripts relacionados ao SCLMDT que podem ser usados por outros produtos. O local real não é especificado em lugar algum. Os arquivos contidos são mantidos pelo administrador do SCLM.
- /var/rdz/pushtoclient/ contém arquivos de configuração de cliente, informações de atualização de produto de cliente e informações de projeto baseado em host, as quais são enviadas ao cliente na conexão com o host. O local real é especificado em pushtoclient.properties (variável pushtoclient.folder). Os arquivos contidos são mantidos por um administrador cliente do Developer for System z.
- /var/rdz/pushtoclient/grouping/ contém os arquivos de configuração de cliente específicos do grupo, informações de atualização do produto de cliente e informações de projeto baseados em host que são enviadas ao cliente na conexão com o host. O local real é especificado em pushtoclient.properties (variável pushtoclient.folder mais o sufixo /grouping). Os arquivos contidos são mantidos por um administrador cliente do Developer for System z.
- /var/rdz/pushtoclient/projects/ mantém os arquivos de definição do projeto baseados em host. O local real é especificado em /var/rdz/pushtoclient/keymapping.xml, que é criado e mantido por um administrador de cliente do Developer for System z. Os arquivos contidos são mantidos por um gerenciador de projetos ou pelo desenvolvedor principal.
- /var/rdz/pushtoclient/install/ contém os arquivos de configuração usados para atualizar a versão do produto de cliente na conexão com o host. O local real é especificado em /var/rdz/pushtoclient/keymapping.xml, que é criado e mantido por um administrador de cliente do Developer for System z. Os arquivos contidos são mantidos por um administrador de cliente do .
- /var/rdz/pushtoclient/install/responsefiles/ contém os arquivos de configuração usados para atualizar a versão do produto de cliente na conexão com o host. O local real é especificado em /var/rdz/pushtoclient/keymapping.xml, que é criado e mantido por um administrador de cliente do Developer for System z. Os arquivos contidos são mantidos por um administrador de cliente do .

Atualizar Privilégios para Administradores que Não São de Sistema

Os dados em `/var/rdz/pushtoclient/` são mantidos por não administradores de sistema, como gerentes de produto, que podem não ter muitos privilégios de atualização no z/OS UNIX. Portanto, é importante entender como o z/OS UNIX configura as permissões de acesso durante a criação de arquivos para assegurar que você tenha uma configuração viável e segura.

Os padrões do UNIX determinam que permissões podem ser configuradas para os três tipos de usuários: proprietário, de grupo e outros. Permissões de leitura, gravação e execução podem ser configuradas para cada tipo individualmente.

O z/OS UNIX configura os UID (user ID) e GID (group ID) para os seguintes valores quando um arquivo é criado:

- O UID é configurado para o UID efetivo do encadeamento de criação.
- O GID é definido para o GID do diretório proprietário. Se o perfil de segurança `FILE.GROUPOWNER.SETGID` estiver definido na classe `UNIXPRIV`, o GID efetivo do encadeamento de criação será usado por padrão. Consulte o *UNIX System Services Planning* (GA22-7800) para obter mais detalhes.

Cada site pode configurar sua própria máscara padrão de permissões de acesso, mas uma máscara comum concede permissão de leitura e de gravação para o proprietário e permissão de leitura para grupos e outros.

Os dados no `/var/rdz/pushtoclient/` são criados usando a máscara de permissões de acesso definida na diretiva `file.permission` do `pushtoclient.properties`. O valor padrão concede permissão de leitura e gravação para o proprietário e grupos e permissão de leitura para outros. Todos têm permissão de execução. As permissões de acesso final devem permitir acesso de leitura e execução a todos, e acesso de gravação aos administradores do cliente do Developer for System z que mantêm os dados.

Os dados em `/var/rdz/pushtoclient/projects/` são criados sem usar nenhuma máscara de permissão de acesso específica. As permissões de acesso final devem conceder permissão de leitura para todos e permissão de gravação para os gerentes de projeto que mantêm os dados.

Comandos de Segurança Úteis

Para assegurar que um grupo de gerentes de projeto ou administradores de cliente do Developer for System z possam gerenciar os dados nesses diretórios, seu administrador de segurança pode ter de criar um grupo com um segmento OMVS válido para eles. Esse grupo é preferivelmente o grupo padrão dos IDs de usuário envolvidos. Consulte *Security Server RACF Command Language Reference* (SA22-7687) para obter mais informações sobre a seguinte amostra de comandos RACF:

```
ADDGROUP RDZPROJ OMVS(GID(1200))
CONNECT IBMUSER GROUP(RDZPROJ)
ALTUSER IBMUSER DFLTGRP(RDZPROJ)
```

Comandos Úteis do z/OS UNIX

Consulte a *UNIX System Services Command Reference* (SA22-7802) para obter mais informações sobre os seguintes comandos de amostra do z/OS UNIX:

- Use o seguinte comando do z/OS UNIX, `ls`, para exibir todos os arquivos em um diretório.

```
ls -lR /var/rdz/pushtoclient/
```

- Use o seguinte comando do z/OS UNIX, **chown**, para alterar o proprietário de um diretório e todos os arquivos que estão nele.

```
chown -R IBMUSER /var/rdz/pushtoclient/
```

- Use o seguinte comando do z/OS UNIX, **chgrp**, para designar o grupo ao diretório e a todos os arquivos que estão nele.

```
chgrp -R RDZPROJ /var/rdz/pushtoclient/
```

- Use o seguinte comando do z/OS UNIX, **chmod**, para fornecer ao proprietário e ao grupo permissão de gravação no diretório e em todos os arquivos contidos nele. A permissão para Outros é de leitura. Todos têm permissão de execução.

```
chmod -R 775 /var/rdz/pushtoclient/
```

Configuração de Amostra

No cenário a seguir, todos os gerentes de projeto de desenvolvimento, uma equipe de três, serão incumbidos de desempenhar tarefas de um administrador cliente do Developer for System z.

O administrador de segurança já designou para a equipe um grupo padrão (RDZPROJ) com um ID de grupo exclusivo (1200). Seus IDs de usuário não possuem privilégios especiais (como UID 0) no z/OS UNIX. O administrador de segurança não definiu o perfil FILE.GROUPOWNER.SETGID. Sendo assim, o z/OS UNIX usará o ID de grupo do diretório ao criar novos arquivos. O ID do usuário IBMUSER (com o UID 0 e o grupo padrão SYS1) foi usado pelo programador de sistemas para criar o diretório `/var/rdz/pushtoclient`.

1. O programador de sistemas limita as permissões de gravação de `/var/rdz/pushtoclient` a proprietários e grupos:

```
# chmod 775 /var/rdz/pushtoclient
# ls -ld /var/rdz/pushtoclient
drwxrwxr-x  2 IBMUSER  SYS1
/var/rdz/pushtoclient
```

Nota: A tarefa FEKSETUP usada durante a configuração da customização já realizou esta etapa.

2. O programador de sistemas torna RDZPROJ o grupo proprietário:

```
# chgrp RDZPROJ /var/rdz/pushtoclient
# ls -ld /var/rdz/pushtoclient
drwxrwxr-x  2 IBMUSER  RDZPROJ
/var/rdz/pushtoclient
```

Isso conclui a configuração necessária para limitar as permissões de gravação de `/var/rdz/pushtoclient` ao programador de sistemas (IBMUSER) e aos gerentes de projeto (RDZPROJ).

Capítulo 2. Considerações de segurança

O Developer for System z fornece acesso ao mainframe para usuários de uma estação de trabalho sem mainframe. A validação dos pedidos de conexão, o fornecimento de comunicação segura entre o host e a estação de trabalho, e a atividade de autorização e auditoria são aspectos importantes da configuração do produto.

Os mecanismos de segurança usados pelos servidores e serviços do Developer for System z dependem dos conjuntos de dados e sistemas de arquivos no qual ele reside sejam seguros. Isto indica que apenas administradores confiáveis de sistema podem ser capazes de atualizar as bibliotecas de programa e os arquivos de configuração.

Os seguintes tópicos são abordados neste capítulo:

- “Métodos de autenticação” na página 20
- “Segurança de conexão” na página 21
- “Usando os PassTickets” na página 23
- “Criação de Log de Auditoria” na página 24
- “Segurança do JES” na página 26
- “Comunicação Criptografada de SSL/TLS” na página 29
- “Autenticação de cliente usando certificados X.509” na página 31
- “Verificação de Port Of Entry (POE)” na página 34
- “Alterando Funções de Cliente” na página 35
- “Grupos de Desenvolvedores de Push-to-client” na página 36
- “Segurança do arquivo de log” na página 37
- “Segurança de Depuração” na página 40
- “segurança do CICSTS” na página 40
- “Segurança de SCLM” na página 41
- “Informações Variadas” na página 41
- “arquivos de configuração do Developer for System z” na página 42
- “Definições de segurança” na página 44

Nota: O Explorador de Sistemas Remotos (RSE), que fornece os principais serviços, como conexão do cliente com o host, consiste em 2 entidades lógicas:

- Daemon RSE, que gerencia a configuração da conexão e que é iniciado como uma tarefa iniciada ou uma tarefa de usuário de longa execução.
- Servidor RSE, que manipula pedidos individuais do cliente e é iniciado como um encadeamento em um ou mais processos-filho pelo daemon RSE.

Consulte Capítulo 1, “Entendendo o Developer for System z”, na página 3 para saber sobre conceitos de design do Developer for System z básicos.

Métodos de autenticação

O Developer for System z suporta diversas formas de autenticar um ID do usuário fornecido por um cliente mediante a conexão.

- ID do Usuário e Senha
- ID do Usuário e Senha Única
- ID do Usuário e Passphrase
- Certificado X.509

Nota: Os dados de autenticação fornecidos pelo cliente só são usados uma vez, durante a configuração de conexão inicial. Depois que um ID do usuário é autenticado, o ID do usuário e os PassTickets autogerados são usados para todas as ações que requerem autenticação.

ID do Usuário e Senha

O cliente fornece um ID de usuário e uma senha correspondente na conexão. O ID de usuário e a senha são usados para autenticar o usuário com seu produto de segurança.

ID do Usuário e Senha Única

Com base em um token exclusivo, uma senha única pode ser gerada por um produto de terceiro. Senhas únicas melhoram a configuração da segurança já que o token exclusivo não pode ser copiado e usado sem o conhecimento do usuário e uma senha interceptada é inútil já que é válida somente uma vez.

O cliente fornece um ID de usuário e a senha única na conexão, que é usada para autenticar o ID do usuário com a saída de segurança fornecida por terceiro. Espera-se que essa saída de segurança ignore os PassTickets usados para satisfazer pedidos de autenticação durante o processamento normal. Os PassTickets devem ser processados por seu software de segurança.

ID do usuário e passphrase

O cliente fornece um ID do Usuário e passphrase correspondente sobre a conexão. O ID e passphrase do usuário são usados para autenticar o usuário com o produto de segurança.

Certificado X.509

Um terceiro pode fornecer um ou mais certificados X.509 que podem ser usados para autenticar um usuário. Quando armazenado em dispositivos seguros, os certificados X.509 combinam uma configuração segura com facilidade de uso para o usuário (nenhum ID do usuário ou senha necessário).

Ao conectar, o cliente fornece um certificado selecionado e, como opção, uma extensão selecionada, que é usada para autenticar o ID do usuário com seu produto de segurança.

Nota: Esse método de autenticação só é suportado pelo método de conexão do daemon RSE, e a comunicação SSL (Secure Socket Layer) deve estar ativada.

Autenticação do JES Job Monitor

A autenticação do cliente é realizada pelo daemon do RSE (ou REXEC/SSH) como parte do pedido de conexão do cliente. Depois de o usuário ser autenticado, os

PassTickets gerados automaticamente são usados para todos os pedidos de autenticação futuros, incluindo o logon automático no JES Job Monitor.

Para que o JES Job Monitor valide o ID do usuário e o PassTicket apresentados pelo RSE, o JES Job Monitor deve ter permissão para avaliar o PassTicket. Isso implica no seguinte:

- Carregue o módulo FEJJMON, por padrão, localizado na biblioteca de carregamento FEK.SFEKAUTH, deve ser autorizado por APF.
- O RSE e o JES Job Monitor devem usar o mesmo ID de aplicativo (APPLID). Por padrão, ambos os servidores usam FEKAPPL como APPLID, mas isso pode ser alterado pela diretiva APPLID em rsed.envvars para RSE e em FEJCNFG para o JES Job Monitor.

Nota: Clientes anteriores (versão 7.0 e mais antiga) comunicam-se diretamente com o JES Job Monitor. Para essas conexões, somente o método de autenticação de ID de usuário e senha é suportado.

Autenticação do Debug Manager

A autenticação do cliente é realizada pelo daemon do RSE (ou REXEC/SSH) como parte do pedido de conexão do cliente. Depois de o usuário ser autenticado, os PassTickets gerados automaticamente são usados para todas as solicitações de autenticação futuras, incluindo o logon automático no Debug Manager.

Para que o Debug Manager valide o ID do usuário e o PassTicket apresentados pelo RSE, o Debug Manager deve ter permissão para avaliar o PassTicket. Isso implica que o módulo de carregamento AQEZPCM, por padrão localizado na biblioteca de carregamento FEK.SFEKAUTH, deve ser autorizado pelo APF.

Quando um Mecanismo de Depuração baseado em cliente se conecta ao Gerenciador de Depuração, ele deve apresentar um token de segurança válido para autenticação.

Segurança de conexão

Diferentes níveis de segurança de comunicação são suportados por RSE, o qual controla a comunicação entre o cliente e a maioria dos serviços do Developer for System z:

- A comunicação externa (cliente-host) pode ser limitada a portas especificadas. Este recurso é desativado por padrão.
- A comunicação externa (cliente-host) pode ser criptografada usando SSL ou TLS. Este recurso é desativado por padrão.
- A verificação de POE (Port Of Entry) pode ser utilizada para permitir acesso ao host apenas a endereços TCP/IP confiáveis. Este recurso é desativado por padrão.

Alguns serviços Developer for System z opcionais usam um caminho de comunicação externo (cliente-host) separado:

- A comunicação do Depurador Integrado pode ser criptografada usando TLS.
- A comunicação do Application Deployment Manager pode ser criptografada usando SSL ao usar a interface Web Services.

O Developer for System z conta com produtos de terceiros, tal como o servidor TN3270, para fornecer alguns serviços. Consulte a documentação do produto relacionada para obter opções de segurança de conexão.

Limitar Comunicação Externa a Portas Especificadas

O programador de sistemas pode especificar as portas nas quais o servidor RSE pode se comunicar com o cliente. Por padrão, qualquer porta disponível é usada. Esse intervalo de portas não possui conexão com a porta do daemon RSE.

Para ajudar a compreender o uso da porta, segue uma breve descrição do processo de conexão do RSE:

1. O cliente se conecta à porta do host 4035, daemon do RSE.
2. O daemon do RSE cria um encadeamento do servidor RSE.
3. O servidor RSE abre uma porta do host para o cliente se conectar. A seleção dessa porta pode ser configurada pelo usuário, no cliente na guia de propriedades do subsistema (isso não é recomendado) ou por meio da definição `_RSE_PORTRANGE` em `rsed.envvars`.
4. O daemon RSE retorna o número da porta para o cliente.
5. O cliente se conecta à porta do host.

Nota:

- O processo é semelhante para o método de conexão alternativo (opcional) usando REXEC/SSH, o qual é descrito em "(Opcional) Usando REXEC (ou SSH)" no *Guia de Configuração do Host* (SC23-7658).
- A porta usada pelo Depurador Integrado e pelo Gerenciador de Implementação de Aplicativos para comunicação externa é definida na configuração de serviço.

Criptografia de Comunicação Usando SSL ou TLS

Todos os fluxos de dados do Developer for System z externos que passam pelo RSE podem ser criptografados usando Secure Socket Layer (SSL) ou Segurança da Camada de Transporte (TLS). O uso de comunicação criptografada é controlado pelas configurações no arquivo de configuração `ssl.properties`, conforme descrito em "Comunicação Criptografada de SSL/TLS" na página 29. A variável `DSTORE_SSL_ALGORITHM` na diretiva `_RSE_JAVA_OPTS` de `rsed.envvars` permite escolher entre SSL e seu TLS sucessor como o método de criptografia, conforme documentado em "Definindo Parâmetros de Inicialização Java Extras com `_RSE_JAVA_OPTS`" no *Guia de Configuração de Host* (SC23-7658).

O Mecanismo de Depurador Integrado no cliente conecta o Gerenciador de Depuração no host. O uso de SSL ou TLS é controlado por uma política Application Transparent TLS (AT-TLS).

O Emulador de Conexão do Host no cliente se conecta a um servidor TN3270 no host. O uso de SSL ou TLS é controlado por TN3270, conforme documentado no *Guia de Configurações de IP do Servidor de Comunicação* (SC31-8775).

Ações remotas (baseadas em host) em subprojetos do z/OS UNIX usam um servidor REXEC ou SSH no host. A comunicação SSH é sempre criptografada usando SSL.

O cliente Application Deployment Manager usa o Serviço da Web CICS TS ou a interface RESTful para chamar os serviços de host do Application Deployment Manager. O uso de SSL é controlado pelo CICS TS, conforme documentado no *RACF Security Guide for CICS TS*.

Verificação de Port Of Entry

O Developer for System z suporta a verificação de Port Of Entry (POE), que permite que o host acesse apenas os endereços TCP/IP confiáveis. O uso de POE é controlado pela definição de perfis específicos em seu software de segurança e a diretiva `enable.port.of.entry` em `rsed.envvars`, conforme descrito em “Verificação de Port Of Entry (POE)” na página 34.

Observe que a ativação de POE afetará outros aplicativos TCPIP que suportam a verificação de POE, como o INETD.

Usando os PassTickets

Após o logon, os PassTickets são usados para estabelecer segurança de encadeamento no servidor RSE. Esse recurso não pode ser desativado. Os PassTickets são senhas geradas pelo sistema com um tempo de vida de aproximadamente 10 minutos. Os PassTickets gerados baseiam-se no algoritmo de criptografia DES, no ID do usuário, no ID do aplicativo, em um registro de data e hora e em uma chave secreta. Essa chave secreta é um número de 64 bits (16 caracteres hexadecimais) que deve ser definido para seu software de segurança. Para segurança adicional, o software de segurança do z/OS trata os PassTickets por padrão como senhas de uso único.

Para ajudá-lo a compreender o uso de PassTicket, a seguir há uma breve descrição do processo de segurança do RSE:

1. O cliente se conecta à porta do host 4035, daemon do RSE.
2. O daemon RSE autentica o cliente usando as credenciais apresentadas pelo cliente.
3. O daemon RSE cria um ID de cliente exclusivo (token de segurança) e um encadeamento de servidor RSE.
4. O servidor RSE gera um PassTicket e cria um ambiente de segurança para o cliente, utilizando o PassTicket como senha.
5. O cliente se conecta à porta do host retornada pelo daemon RSE.
6. O servidor RSE valida o cliente utilizando o ID do cliente.
7. O servidor RSE utiliza um PassTicket recém-gerado como senha para todas as ações futuras que requerem uma senha.

Nota: Um mecanismo similar é usado para configurar conexões seguras com o Debug Manager.

A senha real do cliente não é mais necessária após a autenticação inicial, pois os produtos de segurança compatíveis com SAF podem avaliar as senhas PassTickets e comuns. O servidor RSE gera e utiliza um PassTicket cada vez que uma senha é solicitada, resultando em uma senha válida (temporária) para o cliente.

O uso de PassTickets permite que o RSE configure um ambiente de segurança específico do usuário à vontade, sem a necessidade de armazenar todos os IDs de usuário e senhas em uma tabela, o que poderia ser comprometido. Ele também permite métodos de autenticação de cliente que não usam senhas reutilizáveis, como certificados X.509.

Os perfis de segurança nas classes APPL e PTKTDATA são necessários para que se possa usar os PassTickets. Esses perfis são específicos do aplicativo e, portanto, não afetam a configuração atual do sistema.

Os PassTickets sendo específicos do aplicativo implicam em o RSE e o JES Job Monitor usarem o mesmo ID de aplicativo (APPLID). Por padrão, ambos os servidores usam FEKAPPL como APPLID, mas isso pode ser alterado pela diretiva APPLID em rsed.envvars para o RSE e em FEJCNFG para o JES Job Monitor.

Não é recomendável usar OMVSAPPL como ID do aplicativo porque ele abrirá a chave secreta para a maioria dos aplicativos do z/OS UNIX. Também não é recomendável usar o ID do aplicativo padrão MVS, que é MVS seguido pelo ID do sistema SMF, porque isto abrirá uma chave secreta para a maioria dos aplicativos MVS (incluindo as tarefa em lote do usuário).

A menor unidade de um registro de data e hora de PassTicket é de 1 segundo. Isso significa que todos os PassTickets gerados em um único segundo pelo mesmo aplicativo para o mesmo ID de usuário serão idênticos. Isso, combinado com o PassTickets de manipulação de software de segurança z/OS, causa um problema para o Developer for System z durante o logon, pois diversos PassTickets serão necessários em um segundo. Portanto, o Developer for System z requer a configuração de um sinalizador nas definições do PassTicket que permitem que os PassTickets gerados sejam reutilizados.

| |
|---|
| Atenção: O pedido de conexão do cliente falhará se os PassTickets não estiverem configurados corretamente. |
|---|

Criação de Log de Auditoria

O Developer for System z suporta a criação de log de auditoria das ações que são gerenciadas pelo daemon RSE. Os logs de auditoria são armazenados como arquivos de texto no diretório de log do daemon, utilizando o formato CSV (Comma Separated Value).

Controle de Auditoria

Várias opções no rsed.envvars influenciam a função de auditoria, como documentado em "Definindo parâmetros de inicialização Java com _RSE_JAVAOPTS" no *Guia de Configuração do Host* (SC23-7658).

- A função de auditoria é ativada/desativada pela opção enable.audit.log.
- Os padrões de auditoria são controlados pelas opções de audit.*.
- O local dos arquivos de log de auditoria é controlado pela opção daemon.log. O caminho completo para os logs de auditoria é daemonlog/server, em que daemonlog é o valor da opção daemon.log.
- A página de códigos usada para gravação do log de auditoria é controlada pela diretiva _RSE_HOST_CODEPAGE, conforme documentado em "rsed.envvars, arquivo de configuração RSE" no *Guia de Configuração do Host* (SC23-7658).

O comando do operador **modify switch** pode ser usado para alternar manualmente para um novo arquivo de log de auditoria, conforme documentado em "Comandos do operador" no *Guia de Configuração do Host* (SC23-7658).

Uma mensagem de aviso é enviada para o console quando o sistema de arquivos que contém os arquivos de log de auditoria estiver em execução com pouco espaço livre. Essa mensagem do console (FEK103E) é repetida regularmente até que o problema de pouco espaço seja resolvido.

Processamento de Auditoria

Um novo arquivo de log de auditoria é iniciado após um momento predeterminado ou quando o comando do operador **modify switch** é emitido. O arquivo de log antigo é salvo como `audit.log.yyyymmdd.hhmmss`, em que `yyymmdd.hhmmss` é a data/registro de data e hora no qual o log foi fechado. A data/registro de data e hora do sistema designados ao arquivo indicam a criação do arquivo de log. A combinação das duas datas mostra o período de tempo abrangido por esse arquivo de log de auditoria.

As diretivas `audit.action*` em `rsed.envvars` permitem que você especifique uma saída de usuário (shell script do z/OS UNIX, z/OS UNIX REXX ou programa do z/OS UNIX) que será chamada pelo RSE quando um log de auditoria for fechado. Essa saída de usuário pode então processar os dados contidos no log de auditoria.

Os arquivos de log de auditoria terão a máscara de bit de permissão (`-rw-r----`), se não for alterada pela diretiva `audit.log.mode` em `rsed.envvars`. Isso significa que o proprietário (UID do z/OS UNIX do daemon RSE) tem acesso de leitura e gravação, enquanto o grupo do proprietário (padrão) tem acesso de leitura. Todas as outras tentativas de acesso serão negadas, a menos que isso seja feito por um superusuário (UID 0) ou alguém com permissão suficiente para o perfil `SUPERUSER.FILESYS` na classe de segurança `UNIXPRIV`.

Dados de Auditoria

As seguintes ações são registradas:

- Acesso ao sistema (conexão, desconexão)
- Acesso ao spool JES (envio, exibição, suspensão, liberação, cancelamento, limpeza)
- Acesso ao conjunto de dados (leitura, gravação, criação, exclusão, renomeação, compactação, migração, rechamada)
- Acesso ao arquivo (leitura, gravação, criação, renomeação)
- Execução de comandos do TSO e z/OS UNIX

Cada ação registrada é armazenada (com uma data/registro de data e hora) utilizando o formato Comma Separated Value (CSV), que pode ser lido por uma ferramenta de automação ou de análise de dados. Por exemplo:

```
yyyy/mm/dd hh:mm:ss.sss,userid,action,dataset_name[,returncode]
[,additional_information]
```

Estatísticas de conjunto de dados e de membro também são registradas quando o arquivo é aberto. Elas são anexadas à linha que documenta a conclusão da ação `READ` e os campos são delimitados com `%n`. Por exemplo:

```
yyyy/mm/dd hh:mm:ss.sss,userid,action,dataset_name,returncode,create%modify%n...
```

Os seguintes atributos são registrados, na ordem listada:

- Data e horário de criação (mm/dd/aaaa hh:mm)
- Data e horário da última modificação (mm/dd/aaaa hh:mm:ss)
- Data e horário do último acesso (mm/dd/aaaa hh:mm:ss)
- Formato do registro (RECFM)
- Indicador de revisão SCLM (N = o número de revisão está configurado, D = o número de revisão não está configurado)
- Número de revisão SCLM
- Caracteres "Hexa Inválidos" incluídos (Y = sim, N = não)

Nota: Caracteres “Bad Hex” requerem que o Developer for System z mapeie serviços, pois eles não sobrevivem uma viagem ao cliente e voltar devido a incompatibilidades de página de código.

- Comprimento de registro lógico (LRECL)
- Tamanho do Arquivo
- Reservado para utilização futura
- Reservado para utilização futura
- ID do usuário
- Proprietário do bloqueio (enfileiramento) deste conjunto de dados ou membro
- Pontos de código de CR (retorno do carro), LF (alimentação de linha) e NL (nova linha) do host e seus caracteres de substituição (disponíveis somente quando se usa um cliente Versão 8.0.3 ou superior)

Segurança do JES

O Developer for System z permite acesso do cliente ao spool do JES através do JES Job Monitor. O servidor fornece limitações de acesso básico, que podem ser estendidas com os recursos de proteção padrão do arquivo de spool de seu produto de segurança. As ações do operador (Suspend, Liberar, Cancelar e Limpar) nos arquivos de spool são feitas através do console EMCS, para o qual é necessário configurar permissões condicionais.

Ações nas Tarefas - Limitações de Destino

O JES Job Monitor não fornece aos usuários do Developer for System z acesso total de operador ao spool do JES. Apenas os comandos Suspend, Liberar, Cancelar e Limpar estão disponíveis e, por padrão, somente para arquivos em spool que pertencem ao usuário. Os comandos são emitidos selecionando a opção apropriada na estrutura de menus do cliente (sem prompt de comandos). O escopo dos comandos pode ser ampliado, utilizando perfis de segurança para definir para quais tarefas os comandos estão disponíveis.

Semelhante ao caractere de ação SDSF **SJ**, o JES Job Monitor também suporta o comando Mostrar JCL para recuperar a JCL que criou a saída de tarefa selecionada e o mostra em uma janela de editor. O JES Job Monitor recupera a JCL do JES, tornando-o uma função útil para situações em que o membro JCL original não é facilmente localizado.

Tabela 1. Comandos do Console do JES Job Monitor

| Ações | JES2 | JES3 |
|-------------|---|---------------|
| Suspend | \$Hx(jobid) with x = {J, S or T} | *F,J=jobid,H |
| Liberar | \$Ax(jobid) with x = {J, S or T} | *F,J=jobid,R |
| Cancelar | \$Cx(jobid) with x = {J, S or T} | *F,J=jobid,C |
| Limpar | \$Cx(jobid),P with x = {J, S or T} | *F,J=jobid,C |
| Mostrar JCL | não aplicável | não aplicável |

Os comandos JES disponíveis listados na Tabela 1 são limitados por padrão às tarefas que pertencem ao usuário. Isto pode ser alterado com a diretiva **LIMIT_COMMANDS**, conforme documentado em "FEJCNFG, JES Arquivo de configuração do monitor de tarefas" no *Guia de Configuração do Host* (SC23-7658).

Tabela 2. Matriz de Permissão do Comando LIMIT_COMMANDS

| LIMIT_COMMANDS | Proprietário da tarefa | |
|-----------------|------------------------|--|
| | Usuário | Outros |
| USERID (padrão) | Permitido | Não permitido |
| LIMITED | Permitido | Permitido somente se for permitido explicitamente por perfis de segurança |
| NOLIMIT | Permitido | Permitido se for permitido pelos perfis de segurança ou quando a classe JESSPOOL não estiver ativa |

O JES utiliza a classe JESSPOOL para proteger os conjuntos de dados SYSIN/SYSOUT. Semelhante a SDSF, o JES Job Monitor estende o uso da classe JESSPOOL para proteger os recursos de tarefas também.

Se LIMIT_COMMANDS não for USERID, o JES Job Monitor consultará se há permissão para o perfil relacionado na classe JESSPOOL, conforme mostrado na tabela a seguir.

Tabela 3. Perfis JESSPOOL Estendidos

| Comando | Perfil JESSPOOL | Acesso Necessário |
|-------------|---------------------------------|-------------------|
| Suspender | nodeid.userid.jobname.jobid | ALTER |
| Liberar | nodeid.userid.jobname.jobid | ALTER |
| Cancelar | nodeid.userid.jobname.jobid | ALTER |
| Limpar | nodeid.userid.jobname.jobid | ALTER |
| Mostrar JCL | nodeid.userid.jobname.jobid.JCL | READ |

Use as seguintes substituições na tabela anterior:

| | |
|---------|---|
| nodeid | O ID do nó NJE do subsistema JES de destino |
| userid | ID do usuário local do proprietário da tarefa |
| jobname | Nome da tarefa |
| jobid | ID da tarefa do JES |

Se a classe JESSPOOL não estiver ativa, existe um comportamento diferente para o valor LIMITED e NOLIMIT de LIMIT_COMMANDS, conforme descrito no "Tabela de matriz de permissão do comando LIMIT_COMMANDS" em "FEJJCNFG, arquivo de Configuração do JES Job Monitor" no *Guia de Configuração do Host* (SC23-7658). O comportamento é idêntico quando JESSPOOL está ativo, já que a classe, por padrão, nega a permissão se um perfil não estiver definido.

Ações nas Tarefas - Limitações de Execução

A segunda fase da segurança de comando em spool do JES, depois de especificar os destinos permitidos, inclui as permissões necessárias para realmente executar o comando do operador. Essa autorização de execução é aplicada pelas verificações de segurança do z/OS e do JES.

Observe que Mostrar JCL não é um comando do operador, como os outros comandos JES Job Monitor (Suspender, Liberar, Cancelar e Limpar), de modo que as limitações na próxima lista não se aplicam porque não há nenhuma verificação de segurança adicional.

O JES Job Monitor emite todos os comandos do operador JES solicitados por um usuário através de um console MCS (EMCS) estendido, cujo nome é controlado com o diretiva CONSOLE_NAME, conforme documentado em "FEJJCNFG, JES Arquivo de configuração do monitor de tarefas" no *Guia de Configuração do Host* (SC23-7658).

O JES Job Monitor permite que você defina quanta autoridade é concedida ao console EMCS com a diretiva `LIMIT_CONSOLE`, conforme o documento no "FEJJCNFG, arquivo de configuração do JES Job Monitor" no *Guia de Configuração do Host* (S517-9094).

Tabela 4. Matriz de Autoridade do Console `LIMIT_CONSOLE`

| <code>LIMIT_CONSOLE</code> | Perfil ativo na classe <code>OPERCMD5</code> | Não há perfil ativo na classe <code>OPERCMD5</code> |
|----------------------------|---|---|
| LIMITED (padrão) | Permitido, se houver permissão do perfil de segurança | Não permitido |
| NOLIMIT | Permitido, se houver permissão do perfil de segurança | Permitido |

Essa configuração permite que o administrador de segurança defina permissões granulares de execução de comandos usando as classes `OPERCMD5` e `CONSOLE`.

- Para utilizar um console EMCS, um usuário deve ter (pelo menos) a autoridade `READ` para o perfil `MVS.MCSOPER.console-name` na classe `OPERCMD5`. Observe que, se nenhum perfil estiver definido, o sistema concederá o pedido de autoridade.
- Para executar um comando do operador JES, um usuário deverá ter autoridade suficiente para o perfil `JES%.**` (ou mais específico) na classe `OPERCMD5`. Observe que, se nenhum perfil estiver definido ou a classe `OPERCMD5` não estiver ativa, o JES causará falha no comando se `LIMIT_CONSOLE=LIMITED` estiver definido no `FEJJCNFG`.
- O administrador de segurança também pode exigir que um usuário utilize o JES Job Monitor ao executar o comando do operador especificando `WHEN(CONSOLE(JMON))` na definição **PERMIT**. A classe `CONSOLE` deverá estar ativa para que esta configuração funcione. Observe que a classe `CONSOLE` estando ativa é suficiente; nenhum perfil é verificado para consoles EMCS.

Supondo que a identidade do servidor JES Job Monitor, criando um console `JMON` a partir de uma sessão do TSO, seja impedida por seu software de segurança. Embora o console possa ser criado, o ponto de entrada é diferente (JES Job Monitor versus TSO). Os comandos JES emitidos a partir desse console falharão na verificação de segurança se a segurança estiver configurada conforme documentado nesta publicação e o usuário não tiver autoridade para comandos JES por outros meios.

Observe que o JES Job Monitor não poderá criar o console quando um comando tiver que ser executado se o nome do console já estiver sendo usado. Para evitar isso, o programador de sistema pode configurar a diretiva `GEN_CONSOLE_NAME=ON` no arquivo de configuração do JES Job Monitor ou o administrador de segurança pode definir perfis de segurança para que os usuários do TSO parem de criar um console. Os comandos de amostra do RACF a seguir impedem que qualquer indivíduo (exceto aqueles permitidos) crie um console TSO ou SDSF:

- `RDEFINE TSOAUTH CONSOLE UACC(NONE)`
- `PERMIT CONSOLE CLASS(TSOAUTH) ACCESS(READ) ID(#userid)`
- `RDEFINE SDSF ISFCMD.ODSP.ULOG.* UACC(NONE)`
- `PERMIT ISFCMD.ODSP.ULOG.* CLASS(SDSF) ACCESS(READ) ID(#userid)`

Nota: Sem autorização para esses comandos do operador, os usuários ainda poderão enviar tarefas e ler a saída da tarefa por meio do JES Job Monitor, se tiverem autoridade suficiente para possíveis perfis que protejam esses recursos (como aqueles das classes `JESINPUT`, `JESJOBS` e `JESSPOOL`).

Consulte o *Security Server RACF Security Administrator's Guide* (SA22-7683) para obter informações adicionais sobre proteção de comandos do operador.

Acesso aos Arquivos de Spool

O JES Job Monitor permite acesso de procura a todos os arquivos em spool, por padrão. Isso pode ser alterado com a diretiva `LIMIT_VIEW`, conforme documentado em "FEJJCENFG, JES Arquivo de configuração do monitor de tarefas" no *Guia de Configuração do Host* (SC23-7658).

Tabela 5. Matriz de permissão de navegação `LIMIT_VIEW`

| LIMIT_VIEW | Proprietário da tarefa | |
|------------------|------------------------|--|
| | Usuário | Outros |
| USERID | Permitido | Não permitido |
| NOLIMIT (padrão) | Permitido | Permitido se for permitido pelos perfis de segurança ou quando a classe JESSPOOL não estiver ativa |

Para limitar os usuários às suas próprias tarefas no spool JES, defina a instrução "`LIMIT_VIEW=USERID`" no arquivo de configuração do JES Job Monitor, FEJJCENFG. Se os usuários precisarem de acesso a um intervalo maior de tarefas, mas não todas, use os recursos de proteção de arquivo de spool padrão do seu produto de segurança, como a classe JESSPOOL.

Ao definir a proteção adicional, lembre-se que o JES Job Monitor utiliza a SAPI (SYSOUT Application Program Interface) para acessar o spool. Isto significa que o usuário precisa de, pelo menos, acesso `UPDATE` aos arquivos de spool, mesmo para a funcionalidade de procura. Esse requisito não se aplicará se você executar o z/OS 1.7 (z/OS 1.8 para JES3) ou superior. Aqui, a permissão `READ` é suficiente para a funcionalidade de procura.

Consulte *Security Server RACF Security Administrator's Guide* (SA22-7683) para obter informações adicionais sobre a proteção do arquivo em spool do JES.

Comunicação Criptografada de SSL/TLS

A comunicação externa (cliente-host) usando RSE pode ser criptografada usando SSL (Secure Socket Layer) ou Transport Layer Security (TLS). Esse recurso é desativado por padrão e é controlado pelas configurações no `ssl.properties`. Consulte "(Opcional) `ssl.properties`, criptografia RSE SSL" no *Guia de Configuração do Host* (SC23-7658).

O daemon RSE e o servidor RSE suportam diferentes mecanismos para armazenar certificados devido a diferenças de arquitetura entre eles. Isso implica que as definições e os certificados SSL são necessários para o daemon RSE e para o servidor RSE. Um certificado compartilhado poderá ser usado se o daemon RSE e o servidor RSE usarem o mesmo método de gerenciamento de certificado.

Tabela 6. Mecanismos de armazenamento de certificado SSL

| Armazenamento de certificado | Criado e gerenciado por | Daemon RSE | Servidor RSE |
|------------------------------|---|------------|--------------|
| conjunto de chaves | produto de segurança compatível com SAF | suportados | suportados |
| banco de dados de chaves | gskkyman do z/OS UNIX | suportados | / |
| keystore | keytool do Java | / | suportados |

Nota: Conjuntos de chaves compatíveis com SAF é o método preferido para gerenciar certificados.

Os conjuntos de chaves compatíveis com SAF podem armazenar a chave privada do certificado no banco de dados de segurança ou usando ICSF (Integrated Cryptographic Service Facility), a interface para o hardware de criptografia do System z.

ICSF é recomendado para o armazenamento de chaves privadas associadas a certificados digitais, porque é uma solução mais segura do que o gerenciamento de chaves privadas não ICSF. O ICSF garante que as chaves privadas sejam criptografadas na chave mestra do ICSF e que o acesso a elas seja controlado por recursos gerais das classes de segurança CSFKEYS e CSFSERV. Além disso, o desempenho operacional é aprimorado, pois o ICSF utiliza o Coprocessador Criptográfico de hardware. Consulte o *Cryptographic Services ICSF Administrator's Guide* (SA22-7521) para obter mais detalhes sobre o ICSF e sobre como controlar quem pode usar chaves e serviços criptográficos.

O daemon RSE utiliza funções SSL do Sistema para gerenciar as comunicações criptografadas por SSL. Isso implica que SYS1.SIEALNKE deve ser controlado pelo programa pelo software de segurança e estar disponível para o RSE por meio de LINKLIST ou da diretiva STEPLIB em rsed.envvars.

O ID do usuário do RSE (stcrse nos comandos de amostra a seguir) precisa de autorização para acessar esse conjunto de chaves e os certificados relacionados quando os conjuntos de chaves compatíveis com SAF são usados para o daemon RSE ou o servidor RSE.

- RDEFINE FACILITY IRR.DIGTCERT.LIST UACC(NONE)
- RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC(NONE)
- PERMIT IRR.DIGTCERT.LIST CLASS(FACILITY) ACCESS(READ) ID(stcrse)
- PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ACCESS(READ) ID(stcrse)
- SETROPTS RACLIST(FACILITY) REFRESH

A variável DSTORE_SSL_ALGORITHM na diretiva _RSE_JAVA_OPTS de rsed.envvars permite escolher entre SSL e seu TLS sucessor como método de criptografia, conforme documentado em "Definindo Parâmetros de Inicialização Java Extras com _RSE_JAVA_OPTS" no *Guia de Configuração de Host* (SC23-7658).

Consulte Capítulo 13, "Configurando o SSL e a Autenticação X.509", na página 183 para obter mais detalhes sobre como ativar o SSL para Developer for System z.

Nota: O cliente e o host do Developer for System z devem ter acesso aos protocolos de criptografia comuns (SSLv3 ou TLS) e às definições do conjunto de cifras comuns para serem capazes de configurar a comunicação criptografada. Para obter informações sobre as definições do conjunto de cifras do Java usadas pelo cliente e o servidor RSE, consulte o site de informações de segurança da tecnologia Java do developerWorks (<http://www.ibm.com/developerworks/java/jdk/security/>). Para obter informações sobre as definições do conjunto de cifras do System SSL usado pelo daemon RSE, consulte *Cryptographic Services System SSL Programming* (SC24-5901).

Por padrão, o daemon RSE conta com os padrões do System SSL para os protocolos de criptografia suportados e as definições do conjunto de cifras. É possível alterar estes padrões especificando as variáveis de ambiente GSK_PROTOCOL_* e GSK_V3_CIPHER_SPECS* em rsed.envvars. Para obter informações nestas variáveis de ambiente, consulte *Cryptographic Services System SSL Programming* (SC24-5901).

Comunicação Criptografada pelo Depurador Integrado

A comunicação externa (cliente-host) com o Debug Manager opcional também pode ser criptografada usando SSL ou TLS. Para fazer a criptografia dessa maneira, crie uma política AT-TLS para a porta usada pelo Debug Manager para comunicação externa, por padrão 5335. Uma política de amostra é fornecida em Figura 9. Consulte Capítulo 14, “Configurando o AT-TLS”, na página 195 para obter detalhes sobre a configuração do AT-TLS (Application Transparent TLS).

```
TTLRule                                RDz_Debug_Manager
{
  LocalPortRange                        5335
  Direction                            Inbound
  TLSGroupActionRef                    grp_Production
  TTLEnvironmentActionRef              RDz_Debug_Manager
}
TTLEnvironmentAction                  RDz_Debug_Manager
{
  HandshakeRole Server
  TLSKeyRingParms
  {
    Keyring dbgmgr.racf # Keyring must be owned by the Debug Manager
  }
}
TLSGroupAction                        grp_Production
{
  TTLEnabled                          On
  Trace                               2
}
```

Figura 9. Política AT-TLS para Debug Manager

Nota: O método de comunicação usado pelo Mecanismo de Depuração no cliente Developer for System z para falar com o Debug Manager no host é por padrão ligado ao método de comunicação usado pelo cliente Developer for System z para conversar com o daemon do RSE. Isso implica que se a criptografia estiver ativada para RSE, supõe-se que ela será ativada para o Debug Manager. No entanto, existem cenários alternativos disponíveis para outras instalações.

Autenticação de cliente usando certificados X.509

O daemon RSE suporta que os próprios usuários se autenticuem com um certificado X.509. Usar a comunicação criptografada SSL é um pré-requisito para essa função, uma vez que é uma extensão para a autenticação de host com um certificado usado no SSL.

O daemon RSE inicia o processo de autenticação de cliente pela validação do certificado de cliente. Alguns aspectos chave que são verificados são as datas de validade do certificado e a fidelidade da Autoridade de Certificação (CA) usada para assinar o certificado. Opcionalmente, também é possível consultar uma Lista de Revogação de Certificado (CRL) (terceiros).

Depois que o daemon RSE valida o certificado, ele é processado para autenticação. O certificado é transmitido a seu produto de segurança para autenticação, a menos que a diretiva `rsed.envvars.enable.certificate.mapping` esteja configurada como `false`, quando o daemon RSE fará a autenticação.

Se bem-sucedido, o processo de autenticação determinará o ID do usuário a ser usado para esta sessão, que é, então, testado pelo daemon do RSE para assegurar que seja útil no sistema host onde o daemon do RSE está em execução.

A última verificação (que é feita para cada mecanismo de autenticação, não apenas certificados X.509) verifica se o ID do usuário tem permissão para usar o Developer for System z.

Se você estiver familiarizado com as classificações de segurança do SSL usadas por TCP/IP, a combinação dessas etapas de validação corresponderão às especificações de “Autenticação de Cliente Nível 3” (a mais alta disponível).

Validação da Autoridade de Certificação (CA)

Parte do processo de validação do certificado inclui verificar se o certificado foi assinado por uma Autoridade de Certificação (CA) de confiança. Para fazer isso, o daemon do RSE deve ter acesso a um certificado que identifique a CA.

Ao usar o banco de dados de chaves **gskkyman** para sua conexão SSL, o certificado da CA deve ser incluído no banco de dados de chaves.

Ao usar um conjunto de chaves SAF (que é o método aconselhado), você deve incluir o certificado da CA em seu banco de dados de segurança como o certificado CERTAUTH com o atributo TRUST ou HIGHTRUST, conforme mostrado neste comando RACF de amostra:

- `RACDCERT CERTAUTH ADD(dsn) HIGHTRUST WITHLABEL('label')`

Observe que a maioria dos produtos de segurança já tem os certificados para as CAs reconhecidas disponíveis em seu banco de dados com um status NOTRUST. Use os comandos RACF de amostra a seguir para listar os certificados de CA existentes e marcar um como confiável com base no rótulo designado a ele.

- `RACDCERT CERTAUTH LIST`
- `RACDCERT CERTAUTH ALTER(LABEL('HighTrust CA')) HIGHTRUST`

Nota: O status HIGHTRUST será necessário se você depender do RACF para autenticar o usuário com base na extensão HostIdMappings do certificado. Consulte o “Autenticação por Software de Segurança” na página 33 para obter informações adicionais.

Quando o certificado da CA for incluído em seu banco de dados de segurança, ele deverá ser conectado ao conjunto de chaves RSE, conforme mostrado neste comando RACF de amostra:

- `RACDCERT ID(stcrse) CONNECT(CERTAUTH LABEL('HighTrust CA')
RING(rdzssl.racf))`

Consulte o *Security Server RACF Command Language Reference* (SA22-7687) para obter informações adicionais sobre o comando **RACDCERT**.

Atenção: Se você depender do daemon RSE em vez de seu software de segurança para autenticar um usuário, deverá tomar cuidado para não confundir as CAs com os status TRUST e HIGHTRUST no conjunto de chaves SAF ou no banco de dados de chaves **gskkyman**. O daemon do RSE não é capaz de diferenciar entre os dois, portanto, os certificados assinados por uma CA com status TRUST será válido para propósitos de autenticação de ID do usuário.

(Opcional) Consulte uma Certificate Revocation List (CRL)

Se desejado, é possível instruir o daemon do RSE para verificar uma ou mais Certificate Revocation Lists (CRL) para incluir segurança extra para o processo de validação. Isso é feito incluindo variáveis de ambiente relacionadas à CRL em `rsed.envvars`.

- `GSK_CRL_SECURITY_LEVEL`
- `GSK_LDAP_SERVER`
- `GSK_LDAP_PORT`
- `GSK_LDAP_USER`

- GSK_LDAP_PASSWORD

Consulte *Cryptographic Services System Secure Sockets Layer Programming* (SC24-5901) para obter informações adicionais sobre essas e outras variáveis de ambiente usadas pelo z/OS System SSL.

Nota: Tome cuidado ao especificar outras variáveis de ambiente do z/OS System SSL (GSK_*) em `rse.envvars`, pois elas podem alterar a maneira como o daemon RSE trata as conexões SSL e a autenticação de certificado.

Autenticação por Software de Segurança

O RACF executa várias verificações para autenticar um certificado e retornar o ID do usuário associado. Observe que outros produtos de segurança podem fazer isso de forma diferente. Consulte a documentação de seu produto de segurança para obter informações adicionais sobre a função `initACEE` usada para realizar a autenticação (modo de consulta).

1. O RACF verifica se o certificado está definido na classe DIGTCERT. Se estiver, o RACF retornará o ID do usuário que estava associado a este certificado quando ele foi incluído no banco de dados RACF.

Os certificados são definidos como RACF usando o comando `RACDCERT`, como no seguinte exemplo:

```
RACDCERT ID(userid) ADD(dsn) TRUST WITHLABEL('label')
```

2. Se o certificado não estiver definido, o RACF verificará para ver se há um filtro de nome de certificado correspondente definido nas classes DIGTNMAP ou DIGTCRIT. Se esse for o caso, retorna o ID do usuário associado ao filtro de correspondência mais específico.

Nota: Aconselha-se não usar filtros de nomes para certificados usados pelo Developer for System z, pois esses filtros mapeiam todos os certificados para um único ID de usuário. O resultado é que todos os usuários do Developer for System z efetuarão login com o mesmo ID do usuário.

3. Se não houver nenhum filtro de nome correspondente, o RACF localizará a extensão de certificado `HostIdMappings` e extrairá o par de ID de usuário e nome do host integrado. Se localizado e validado, o RACF retornará o ID do usuário definido na extensão `HostIdMappings`.

O par ID do usuário e nome do host é válido se todas estas condições forem verdadeiras:

- O certificado da CA usado para assinar esse certificado é marcado como `HIGHTRUST` na classe DIGTCERT.
- O ID do usuário armazenado na extensão tem um comprimento válido (1 a 8 caracteres).
- O ID do usuário designado ao daemon do RSE tem (pelo menos) autoridade `READ` para o perfil `IRR.HOST.hostname` na classe `SERVAUTH`, onde `hostname` é o nome do host armazenado na extensão. É geralmente um nome de domínio, como `CDFMVS08.RALEIGH.IBM.COM`.

A definição da extensão `HostIdMappings` na sintaxe ASN.1 é:

```
id-ce-hostIdMappings OBJECT IDENTIFIER ::= { 1 3 18 0 2 18 1 }
HostIdMappings ::= SET OF HostIdMapping
HostIdMapping ::= SEQUENCE {
    hostName      IMPLICIT[1] IA5String,
    subjectId     IMPLICIT[2] IA5String,
    proofOfIdPossession IdProof OPTIONAL
}
IdProof ::= SEQUENCE {
    secret        OCTET STRING,
    encryptionAlgorithm OBJECT IDENTIFIER
}
```

Nota: Uma extensão HostIdMappings não é honrada se o ID do usuário de destino tiver sido criado após o início do período de validade para o certificado contendo a extensão HostIdMappings. Portanto, se você estiver criando IDs de usuários especificamente para certificados com extensões HostIdMappings, certifique-se de que você tenha criado os IDs de usuários antes de os pedidos de certificados serem enviados.

Consulte o Guia de Administrador de Segurança para o *Servidor de Segurança RACF* (SA22-7683) para obter mais informações em certificados X.509, como eles são gerenciados pelo RACF, e como definir filtros de nomes de certificados. Consulte o *Security Server RACF Command Language Reference* (SA22-7687) para obter informações adicionais sobre o comando **RACDCERT**.

Autenticação por Daemon do RSE

Developer for System z podem fazer autenticação de certificado X.509 básica sem contar com seu produto de segurança. A autenticação realizada pelo daemon do RSE requer que um ID do usuário e nome do host sejam definidos em uma extensão de certificado e está ativa somente se a diretiva `enable.certificate.mapping` em `rsed.envvars` estiver configurada para `FALSE`.

Essa função deverá ser usada se o seu produto de segurança não suportar autenticação de um usuário com base em um certificado X.509 ou se o seu certificado for causar falha no(s) teste(s) feito(s) por seu produto de segurança (por exemplo, o certificado possui um identificador falho para a extensão HostIdMappings e não há nenhum filtro ou definição em DIGTCERT).

O cliente consultará o usuário pelo identificador da extensão (OID) a ser usado, que é, por padrão, o OID de HostIdMappings, {1 3 18 0 2 18 1}.

O daemon do RSE extrairá o ID do usuário e o nome do host do mesmo usando o formato da extensão HostIdMappings. Esse formato está descrito em “Autenticação por Software de Segurança” na página 33.

O par ID do usuário e nome do host é válido se todas estas condições forem verdadeiras:

- O ID do usuário armazenado na extensão tem um comprimento válido (1 a 8 caracteres).
- O ID do usuário designado ao daemon do RSE tem (pelo menos) autoridade `READ` para o perfil `IRR.HOST.hostname` na classe `SERVAUTH`, onde `hostname` é o nome do host armazenado na extensão. É geralmente um nome de domínio, como `CDFMVS08.RALEIGH.IBM.COM`.

Atenção: Depende do administrador de segurança assegurar que todas as CAs conhecidas do daemon RSE sejam altamente confiáveis, já que o daemon RSE não pode verificar se aquele que assinou o certificado de cliente é altamente confiável ou apenas confiável. Consulte “Validação da Autoridade de Certificação (CA)” na página 32 para obter informações adicionais sobre certificados de CA acessíveis.

Verificação de Port Of Entry (POE)

O Developer for System z suporta a verificação de Port Of Entry (POE), que permite que o host acesse apenas os endereços TCP/IP confiáveis. Esse recurso fica desativado por padrão e requer a definição do perfil de segurança `BPX.POE`, conforme mostrado nos seguintes comandos RACF de amostra:

- `RDEFINE FACILITY BPX.POE UACC(NONE)`
- `PERMIT BPX.POE CLASS(FACILITY) ACCESS(READ) ID(STCRSE)`

- SETROPTS RACLIST(FACILITY) REFRESH

Nota:

- O RSE deve ser configurado para usar o POE removendo-se o comentário da opção “enable.port.of.entry=true” em `rsed.envvars`, conforme documentado em “Definindo parâmetros de inicialização Java com `_RSE_JAVAOPTS`” no *Guia de Configuração do Host* (SC23-7658).
- O ID de usuário do RSE STCRSE requer o UID(0) quando esse perfil não está definido e a verificação de POE está ativada em `rsed.envvars`.
- A definição de BPX.POE afetará outros aplicativos TC/PIP que suportam a verificação de POE, como INETD.
- As zonas de segurança (perfis EZB.NETACCESS.**, que são os intervalos de endereços IP) devem ser configuradas na classe SERVAUTH para utilizar toda a força da verificação de POE.

Consulte o *Communications Server IP Configuration Guide* (SC31-8775) para obter informações adicionais sobre o controle de acesso à rede usando a verificação de POE.

Alterando Funções de Cliente

Clientes do Developer for System z versão 8.5.1 e mais recente podem verificar a autorização de acesso aos perfis de segurança do SAF, e baseado no resultado, ativar ou desativar a função relacionada para o usuário.

Developer for System z verifica permissões de acesso aos perfis listados em Tabela 7 para determinar quais opções devem ser ativadas ou desativadas para o usuário.

Tabela 7. Informações de SAF para Alterar Funções de Cliente

| Perfil FACILITY | Comprimento fixo | Acesso Necessário | Resultado |
|------------------------------------|------------------|-------------------|--|
| FEK.USR.OFF.REMOTECOPY.MVS.sysname | 27 | READ | O cliente desativa funções de copiar e relacionadas para conjuntos de dados do MVS |

Nota: O Developer for System z presume que um usuário não tenha autorização de acesso quando o software de segurança indica que ele não pode determinar se um usuário tem ou não autorização de acesso a um perfil. Um exemplo disso é quando o perfil não está definido.

O valor `sysname` corresponde ao nome do sistema de destino.

A coluna “Comprimento fixo” documenta o comprimento da parte fixa do perfil de segurança relacionado.

Por padrão, o Developer for System z espera os perfis FEK.* estarem na classe de segurança FACILITY. Observe que os perfis na classe FACILITY estão limitados a 39 caracteres. Se a soma do comprimento da parte do perfil fixo (FEK.USR.<key>) e o comprimento da parte do perfil específica do site (sysname) exceder este número, é possível posicionar os perfis em outra classe e instrui o Developer for System z a usar esta classe no lugar. Para fazer isso, remova o comentário da linha `_RSE_FEK_SAF_CLASS` em `rsed.envvars` e forneça o nome de classe desejado.

As seguintes definições de segurança de amostra permitem a ação REMOTECOPY.MVS para todos os usuários no CDFMVS08, exceto aqueles no grupo RESTRICT:

```
RDEFINE FACILITY (FEK.USR.OFF.REMOTECOPY.MVS.CDFMVS08) -
  UACC(NONE) DATA('RATIONAL DEVELOPER FOR SYSTEM Z - CLIENT CONTROL')
PERMIT FEK.USR.OFF.REMOTECOPY.MVS.CDFMVS08 CLASS(FACILITY) -
  ID(RESTRICT) ACCESS(READ)
SETROPTS RACLIST(FACILITY) REFRESH
```

OFF.REMOTECOPY.MVS

Quando os usuários tiverem acesso de LEITURA ao perfil FEK.USR.OFF.REMOTECOPY.MVS.sysname, então seus clientes do Developer for System z versão 8.5.1 e mais recente desativarão as ações arrastar, copiar, salvar como e trabalhar offline para os conjuntos de dados MVS. O resultado é que os usuários podem acessar os conjuntos de dados nesse sistema, mas os usuários não podem criar uma cópia local de um conjunto de dados em sua estação de trabalho. Isso ajuda a evitar a exposição de informações confidenciais se a estação de trabalho local for perdida ou roubada.

Grupos de Desenvolvedores de Push-to-client

Os clientes do Developer for System z versão 8.0.1 e superior podem extrair arquivos de configuração de cliente e informações de upgrade do host quando se conectam, assegurando que todos os clientes tenham configurações comuns e estejam atualizados.

Desde a versão 8.0.3, o administrador de cliente pode criar diversos conjuntos de configuração de cliente e diversos cenários de atualização de cliente para ajustar as necessidades de diferentes grupos de desenvolvedores. Isso permite que os usuários recebam uma configuração customizada, com base em critérios como associação de um grupo LDAP ou permissão para um perfil de segurança.

Ao usar as definições do banco de dados de segurança como mecanismo de seleção (o valor SAF é especificado para diretivas em pushtoclient.properties), o Developer for System z verifica as permissões de acesso aos perfis listados na Tabela 8 para determinar a quais grupos de desenvolvedores o usuário pertence, e se um usuário tem permissão para rejeitar atualizações.

Tabela 8. Informações do SAF de Push-to-client

| Perfil FACILITY | Comprimento fixo | Acesso Necessário | Resultado |
|---|------------------|-------------------|---|
| FEK.PTC.CONFIG.ENABLED. sysname.devgroup | 23 | READ | O cliente aceita atualizações de configuração para o grupo especificado |
| FEK.PTC.PRODUCT. ENABLED.sysname.devgroup | 24 | READ | O cliente aceita atualizações de produto para o grupo especificado |
| FEK.PTC.REJECT.CONFIG. UPDATES.sysname[.devgroup] | 30 | READ | O usuário pode rejeitar atualizações de configuração |
| FEK.PTC.REJECT.PRODUCT. UPDATES.sysname[.devgroup] | 31 | READ | O usuário pode rejeitar atualizações de produto |

Nota: O Developer for System z presume que um usuário não tenha autorização de acesso quando o software de segurança indica que ele não pode determinar se um usuário tem ou não autorização de acesso a um perfil. Um exemplo disso é quando o perfil não está definido.

O valor devgroup corresponde ao nome do grupo designado a um grupo específico de desenvolvedores. Observe que o nome do grupo é visível nos clientes do Developer for System z.

O valor `sysname` corresponde ao nome do sistema de destino.

A coluna “Comprimento fixo” documenta o comprimento da parte fixa do perfil de segurança relacionado.

Por padrão, o Developer for System z espera os perfis FEK.* estarem na classe de segurança FACILITY. Observe que os perfis na classe FACILITY estão limitados a 39 caracteres. Se a soma do comprimento da parte do perfil fixado (FEK.PTC.<key>) e o comprimento da parte do perfil específico do site (`sysname` ou `sysname.devgroup`) exceder este número, será possível colocar os perfis em outra classe e instruir o Developer for System z para usar esta classe no lugar. Para fazer isso, remova o comentário da linha `_RSE_FEK_SAF_CLASS` em `rsed.envvars` e forneça o nome de classe desejado.

Observe que o administrador de cliente deve estar na lista de acesso dos perfis FEK.PTC.*.ENABLED.* para definir e gerenciar os metadados de push-to-client relacionados. Isso significa que os perfis devem ser definidos com (pelo menos) o administrador de cliente na lista de acesso para que o push-to-client com suporte de grupo possa ser implementado.

Consulte “(Opcional) `pushtoclient.properties`, Controle de Cliente Baseado em Host” no *Guia de Configuração do Host* (S517-9094) para obter mais informações sobre como ativar o suporte a diversos grupos. Consulte Capítulo 7, “Considerações de Push-to-client”, na página 119 para obter mais informações sobre conceitos e implementação de push-to-client.

Segurança do arquivo de log

Criação de log

Os diretórios de log e os arquivos de log criados por Developer for System z têm, por padrão, permissões de acesso seguro aos locais em que o proprietário possui acesso (de leitura ou gravação). Para os logs de servidor (e de auditoria), o proprietário é o ID do usuário da tarefa RSED iniciada. Para os logs de usuário, o proprietário é o ID do usuário fornecido pelo usuário final durante o logon. A diretiva `log.file.mode` em `rsed.envvars` pode ser usada para configurar permissões de acesso diferentes. Observe que as permissões de acesso para os arquivos de auditoria são controladas separadamente, e elas são configuradas com a diretiva `audit.log.mode` em `rsed.envvars`.

Antes de gravar em um diretório de log, Developer for System z validará a propriedade do arquivo e falhará na gravação se um usuário diferente possuir o arquivo. Esse comportamento é novo na versão 9.1.0 e pode requerer mudanças em uma estrutura de arquivo de log existente. A diretiva `log.secure.mode` no `rsed.envvars` pode ser usada para desativar a verificação de propriedade.

A amostra JCL FEKPBITS pode ser usada para converter as permissões de acesso e propriedade de uma infraestrutura de arquivo de log existente. O FEKPBITS está localizado no FEK.#CUST.JCL, a menos que você tenha especificado um local diferente ao customizar e enviar a tarefa FEK.SFEKSAMP(FEKSETUP). Consulte “Instalação de Customização” no *Guia de Configuração de Host* (SC23-7658) para obter mais detalhes.

Coleção de logs – requisitos para o solicitante

A tarefa de iniciação do RSED suporta o comando do operador **MODIFY LOGS** para coletar logs de host e informações de configuração do Developer for System z. Os dados coletados são colocados em um arquivo z/OS UNIX, \$TMPDIR/feklogs%sysname.%jobname, em que \$TMPDIR é o valor da diretiva TMPDIR em rsed.envvars (/tmp padrão), %sysname é seu nome do sistema z/OS e %jobname é o nome da tarefa iniciada do RSED.

Developer for System z consultará seu produto de segurança para as permissões de acesso dos perfis do FEK.CMD.LOGS.** a fim de determinar se ao solicitante é permitido coletar os logs especificados. Por padrão, o solicitante é o ID do usuário da tarefa iniciada do RSED, a menos que a opção OWNER seja especificada. Apenas o solicitante possui acesso ao arquivo que está mantendo os dados coletados.

| Perfil FACILITY | Comprimento fixo | Acesso Necessário | Resultado |
|-----------------------------|------------------|-------------------|--|
| FEK.CMD.LOGS.AUDIT.jobname | 19 | READ | O solicitante pode coletar logs de auditoria do nome da tarefa |
| FEK.CMD.LOGS.SERVER.jobname | 20 | READ | O solicitante pode coletar logs do servidor do nome da tarefa |
| FEK.CMD.LOGS.USER.userid | 18 | READ | O solicitante pode coletar logs de usuário do ID do usuário |
| FEK.CMD.LOGS.OWNER.userid | 19 | READ | O solicitante é alterado a partir do ID do usuário da tarefa iniciada do RSED para o ID do usuário |

Nota: O Developer for System z presume que um usuário não tenha autorização de acesso quando o software de segurança indica que ele não pode determinar se um usuário tem ou não autorização de acesso a um perfil. Um exemplo disso é quando o perfil não está definido.

O valor jobname corresponde ao nome da tarefa iniciada do RSED. O valor userid corresponde a um ID de usuário válido

A coluna “Comprimento fixo” documenta o comprimento da parte fixa do perfil de segurança relacionado.

Por padrão, o Developer for System z espera os perfis FEK.* estarem na classe de segurança FACILITY. Observe que os perfis na classe do FACILITY são limitados para 39 caracteres. Se a soma do comprimento da parte do perfil fixado (FEK.CMD.LOGS.<key>) e o comprimento da parte do perfil específico do site (jobname ou userid) exceder este número, será possível colocar os perfis em outra classe e instruir o Developer for System z a usar esta classe, em vez disso. Para fazer isso, remova o comentário da linha _RSE_FEK_SAF_CLASS em rsed.envvars e forneça o nome de classe desejado.

Violações de acesso são reportadas com a mensagem do console FEK302E.

As definições de segurança de amostra a seguir permitem que todos coletem logs de host, mas apenas o grupo SYSPROG pode coletar dados de auditoria:

```
RDEFINE FACILITY (FEK.CMD.LOGS.** ) UACC(READ) -  
  DATA('RATIONAL DEVELOPER FOR SYSTEM Z - LOGS OPERATOR COMMAND')  
RDEFINE FACILITY (FEK.CMD.LOGS.AUDIT.** ) UACC(NONE) -  
  DATA('RATIONAL DEVELOPER FOR SYSTEM Z - LOGS OPERATOR COMMAND')  
PERMIT FEK.CMD.LOGS.AUDIT.** CLASS(FACILITY) -  
  ID(SYSPROG) ACCESS(READ)  
SETROPTS RACLIST(FACILITY) REFRESH
```


Coleção de logs – requisitos para o solicitante

O comando do operador **MODIFY LOGS** usa o ID do usuário da tarefa iniciada do RSED para coletar logs de host e informações de configuração, e, por padrão, arquivos de log de usuário são criados com permissões de acesso de arquivo seguro (apenas o proprietário possui acesso). Para ser capaz de coletar arquivos de log de usuários seguros, o ID do usuário da tarefa iniciada do RSED deve ter permissão para lê-los.

O argumento **OWNER** do comando do operador **MODIFY LOGS** resulta no ID do usuário especificado se tornar o proprietário dos dados coletados. A fim de alterar a propriedade, ao ID do usuário da tarefa inicial do RSED deve ser permitido usar o serviço **CHOWN** z/OS UNIX.

Há três maneiras nas quais estas permissões podem ser fornecidas para o ID do usuário da tarefa iniciada do RSED. Em ordem de preferência, são elas

- Acesso para selecionar perfis na classe **UNIXPRIV**. Este método é usado na tarefa de amostra **FEKRACF**.
- Acesso ao perfil **BPX.SUPERUSER** na classe **FACILITY**
- **UID 0**

Permissões de classe **UNIXPRIV**

A classe **UNIXPRIV** retém perfis que permitem que um administrador de segurança entregue seletivamente as permissões especiais relacionadas ao z/OS UNIX, em vez de conceder todas as permissões relacionadas ao z/OS UNIX com a abordagem do super usuário.

*Tabela 9. Permissões relacionadas ao **UNIXPRIV** z/OS UNIX*

| Perfil | Permissão | Resultado |
|--------------------------------------|-------------|---|
| SUPERUSER.FILESYS | READ | Ao usuário é permitido ler qualquer arquivo ou diretório. |
| SUPERUSER.FILESYS.ACLOVERRIDE | READ | A permissão só é necessária se o ACLOVERRIDE já estiver definido. Ele permite ao usuário ler qualquer arquivo ou diretório, independente das definições ACL . |
| SUPERUSER.FILESYS.CHOWN | READ | É permitido que o usuário altere o proprietário de qualquer arquivo ou diretório. |

Nota: Quando o perfil do **SUPERUSER.FILESYS.ACLOVERRIDE** for definido, as permissões de acesso definidas no **ACL** (Lista de Controle de Acesso) têm precedência sob as permissões concedidas por meio do **SUPERUSER.FILESYS**. O ID do usuário da tarefa iniciada do RSED precisará da permissão de acesso **READ** para o arquivo **SUPERUSER.FILESYS.ACLOVERRIDE** para efetuar bypass nas definições **ACL**.

Permissão do perfil **BPX.SUPERUSER**

Quando o ID do usuário da tarefa iniciada do RSED possui permissão de **READ** para o perfil **BPX.SUPERUSER** na classe **FACILITY**, ele também é capaz de se tornar temporariamente um super usuário do z/OS UNIX, para o qual as permissões de acesso ao arquivo z/OS UNIX não contam.

UID 0

Quando o ID do usuário da tarefa iniciada do RSED possui **UID 0** especificado em seu segmento **OMVS**, ele é um super usuário z/OS UNIX, para o qual as permissões de acesso do arquivo z/OS UNIX não se aplicam. Entretanto, essa abordagem não é aconselhável, já que o **UID 0** é provavelmente um **UID** compartilhado e é recomendável para dar ao ID do usuário da tarefa iniciada do

RSED um UID exclusivo devido a outras permissões concedidas ao ID. (Por exemplo, os administradores do z/OS UNIX requerem UID 0 para determinadas tarefas de gerenciamento de sistema.)

Segurança de Depuração

O Integrated Debugger opcional requer que usuários tenham permissões de acesso suficiente para perfis de segurança especificados. Se o usuário não tiver a permissão necessária, a sessão de depuração não será iniciada.

O Developer for System z verifica o acesso aos perfis listados em Tabela 10 para determinar quais permissões de depuração foram concedidas.

Tabela 10. Informações de SAF para Funções de Depuração

| Perfil FACILITY | Acesso Necessário | Resultado |
|-----------------------|-------------------|--|
| AQE.AUTHDEBUG.STDPGM | READ | Usuário é capaz de depurar aplicativos de estado de problema |
| AQE.AUTHDEBUG.AUTHPGM | READ | Usuário é capaz de depurar aplicativos de estado de problema e autorizados |

Nota:

- O Developer for System z presume que um usuário não tenha autorização de acesso quando o software de segurança indica que ele não pode determinar se um usuário tem ou não autorização de acesso a um perfil. Um exemplo disso é quando o perfil não está definido.
- versões do Developer for System z anteriores à versão 9.1.1 verificadas para permissão de UPDATE para o perfil AQE.AUTHDEBUG.WRITEBUFFER para permitir a depuração de transações de CICS de somente leitura. Este perfil não é mais usado e pode ser removido se o seu sistema host tiver somente Developer for System z versão 9.1.1 ou superior.

As seguintes definições de segurança de amostra permitem que todos os usuários em grupo RDZDEBUG depurem aplicativos de estado de problema:

```
DEFINE FACILITY (AQE.AUTHDEBUG.STDPGM) -  
  UACC(NONE) DATA('RATIONAL DEVELOPER FOR SYSTEM Z - DEBUG PROBLEM-STATE')  
PERMIT AQE.AUTHDEBUG.STDPGM CLASS(FACILITY) -  
  ID(RDZDEBUG) ACCESS(READ)  
SETROPTS RACLIST(FACILITY) REFRESH
```

segurança do CICSTS

O Depurador Integrado opcional é capaz de depurar transações CICS. Consulte “Depuração de Transação do CICS” na página 147 para obter mais detalhes.

O Developer for System z permite, através do Application Deployment Manager, que administradores do CICS controlem quais definições de recurso do CICS podem ser editadas pelo desenvolvedor, seus valores-padrão e a exibição de uma definição de recurso do CICS por meio de um servidor CICS Resource Definition (CRD). Consulte Capítulo 8, “considerações CICSTS”, na página 137 para obter informações adicionais sobre as definições de segurança necessárias do CICS TS.

repositório do CRD

O conjunto de dados de VSAM do repositório do servidor CRD contém todas as definições de recurso padrão e deve, portanto, ser protegido contra atualizações, mas os desenvolvedores devem ter permissão para ler os valores armazenados aqui.

transações do CICS

O Developer for System z fornece várias transações que são usadas pelo servidor CRD durante a definição e a consulta de recursos do CICS. Quando a transação é conectada, a verificação de segurança de recurso do CICS, se ativada, garante que o ID do usuário esteja autorizado para executar o ID de transação.

comunicação criptografada por SSL

O cliente Application Deployment Manager usa os Serviços da Web do CICS TS ou a interface RESTful para chamar o servidor CRD. O uso de SSL para essa comunicação é controlado pela definição TCPIPService do CICS TS, conforme documentado no *RACF Security Guide for CICS TS*.

Segurança de SCLM

O serviço SCLM Developer Toolkit oferece funcionalidade de segurança opcional para as funções Construir, Promover e Implementar.

Se a segurança for ativada para uma função pelo administrador de SCLM, as chamadas SAF serão feitas para verificar a autoridade para executar a função protegida com o ID do usuário do responsável pela chamada ou do substituto.

Consulte *SCLM Developer Toolkit Administrator's Guide* (SC23-9801), para obter informações adicionais sobre as definições de segurança SCLM necessárias.

Informações Variadas

Lixeira GATE

A primeira vez que um espaço de endereço instrui o RACF a acessar uma classe de recurso que não é RACLISTed (armazenada na memória), como a classe DATASET, o RACF recuperará e armazenará todos os perfis genéricos no espaço de endereço do usuário, em uma lista conhecida como GATE (Generic Anchor Table Entry). Até o z/OS 1.12, RACF mantém quatro âncoras genéricas para cada espaço de endereço e quatro para cada MVS TCB que tem seu próprio ACEE. Quando todos os quatro forem usados, RACF substituirá o menos recentemente mencionado quando um novo entrar.

Se seus usuários acessam frequentemente mais de quatro qualificadores de alto nível de conjunto de dados, os conjuntos de encadeamentos RSE (que atendem a diversos usuários usando encadeamentos com ACEEs específicos ao usuário) poderão passar pela lixeira GATE pois RACF tem de rotear novas entradas por meio dos slots de âncora disponíveis.

Em z/OS 1.12, RACF introduziu a opção **GENERICANCHOR** do comando **SET**, que permite aumentar o tamanho da tabela. Isso pode ser configurado em todo o sistema para cada nome de tarefa.

ACEE Gerenciado

O Developer for System z usa os serviços kernel do z/OS UNIX, como `pthread_security_np()` e `__passwd()`, que usam o serviço de segurança InitACEE, resultando em blocos de controle de segurança "ACEE gerenciado". Um ACEE (Elemento de Ambiente do Acessador) gerenciado é armazenado em cache pelo produto de segurança, e o produto de segurança ignorará determinadas mudanças

(como mudanças de senha fora do Developer for System z) até que o cache atinja o tempo limite. (O esgotamento do tempo limite pode levar vários minutos.)

Atualize o cache do ACEE gerenciado após as mudanças de segurança para garantir que os novos dados sejam usados pelo Developer for System z.

Armazenamento em cache do ACEE

O RACF pode salvar ACEEs (Accessor Environment Elements) usando VLF (Virtual Lookaside Facility) e os recupera para uso posterior. O Developer for System z solicita que o software de segurança construa diversos ambientes de segurança (ACEEs) para o mesmo usuário (um para cada encadeamento específico do usuário no conjunto de encadeamentos RSE) e pode assim se beneficiar com o armazenamento em cache do ACEE.

Para obter mais informações sobre armazenamento em cache do ACEE, consulte “Considerações de ACEEs e VLF” no *Guia do Programador do Sistema RACF do Servidor de Segurança (SA22-7681)*.

arquivos de configuração do Developer for System z

Há vários arquivos de configuração do Developer for System z cujas diretivas impactam a segurança e a configuração de auditoria. Com base nas informações deste capítulo, o administrador de segurança e o programador de sistemas podem decidir quais devem ser as configurações para as diretivas a seguir.

JES Job Monitor - FEJJC�FG

- `LIMIT_COMMANDS={USERID | LIMITED | NOLIMIT }`
Definir em relação a quais ações as tarefas podem ser realizadas (excluindo navegação e envio). Para obter mais informações, consulte “Ações nas Tarefas - Limitações de Destino” na página 26.
- `LIMIT_CONSOLE={LIMITED | NOLIMIT}`
Defina o nível de autoridade do console EMCS usado para executar as ações. Para obter mais informações, consulte “Ações nas Tarefas - Limitações de Destino” na página 26.
- `LIMIT_VIEW={USERID | NOLIMIT}`
Definir quais arquivos de spool podem ser navegados. Para obter mais informações, consulte “Acesso aos Arquivos de Spool” na página 29.
- `LOOPBACK_ONLY={ON | OFF}`
Defina se o JES Job Monitor pode ser acessado fora do sistema z/OS. Para obter mais informações, consulte a seção *Arquivo de configuração FEJJC�FG, JES Job Monitor* no capítulo *Customização básica do Guia de Configuração de Host (S517-9094)*.
- `APPLID={FEKAPPL | *}`
ID do aplicativo usado para criação/validação do PassTicket. Para obter informações adicionais, consulte “Usando os PassTickets” na página 23.

Nota: Detalhes sobre essas e outras diretivas FEJJC�FG estão disponíveis em “FEJJC�FG, JES Arquivo de configuração do monitor de tarefas” no *Guia de Configuração do Host (SC23-7658)*.

RSE - rsed.envvars

- `_RSE_FEK_SAF_CLASS={FACILITY | *}`

Perfis FEK.** de participação da classe de segurança. Para obter mais informações, consulte “Grupos de Desenvolvedores de Push-to-client” na página 36 e “Alterando Funções de Cliente” na página 35.

- (_RSE_JAVAOPTS) -DDENY_PASSWORD_SAVE={true | false}

Nega aos usuários o salvamento de sua senha do host no cliente. Para obter informações adicionais, consulte “Definindo parâmetros de inicialização Java com _RSE_JAVAOPTS” no *Guia de Configuração do Host* (SC23-7658).

- (_RSE_JAVAOPTS) -DDSTORE_IDLE_SHUTDOWN_TIMEOUT=value

Cronômetro para desconectar clientes inativos. Para obter informações adicionais, consulte “Definindo parâmetros de inicialização Java com _RSE_JAVAOPTS” no *Guia de Configuração do Host* (SC23-7658).

- (_RSE_JAVAOPTS) -DAPPLID={FEKAPPL | *}

ID do aplicativo usado para criação/validação do PassTicket. Para obter informações adicionais, consulte “Usando os PassTickets” na página 23.

- (_RSE_JAVAOPTS) -Denable.port.of.entry={true | false}

Ativar a verificação de Porta de Entrada. Para obter informações adicionais, consulte “Verificação de Port Of Entry (POE)” na página 34.

- (_RSE_JAVAOPTS) -DDSTORE_SSL_ALGORITHM={TLSv1.2 | SSL}

Selecione SSL ou TLS como o método de criptografia de comunicação. Para obter informações adicionais, consulte “Comunicação Criptografada de SSL/TLS” na página 29.

- (_RSE_JAVAOPTS) -Denable.certificate.mapping={true | false}

Use o seu produto de segurança para autenticar usuários com um certificado X.509. Para obter informações adicionais, consulte “Autenticação de cliente usando certificados X.509” na página 31.

- GSK_CRL_SECURITY_LEVEL={LOW | MEDIUM | HIGH}

```
GSK_LDAP_SERVER=*
GSK_LDAP_PORT={389 | *}
GSK_LDAP_USER=*
GSK_LDAP_PASSWORD=*
```

Verificações de segurança adicional para autenticação do X.509. Para obter informações adicionais, consulte “(Opcional) Consulte uma Certificate Revocation List (CRL)” na página 32.

- (_RSE_JAVAOPTS) -Dlog.file.mode={RW.N.N | * }

A máscara da permissão de acesso a arquivos e diretórios de log de host.

- (_RSE_JAVAOPTS) -Dlog.secure.mode={true | false }

A segurança adicional verifica (como propriedade) para arquivos e diretórios de log de host.

- (_RSE_JAVAOPTS) -Ddaemon.log={/var/rdz/logs | * }

Liderança de caminho para os arquivos de log de auditoria. Para obter informações adicionais, consulte “Criação de Log de Auditoria” na página 24.

- (_RSE_JAVAOPTS) -Daudit.log.mode={RW.R.N | * }

Máscara de permissões de acesso dos arquivos de log de auditoria. Para obter informações adicionais, consulte “Criação de Log de Auditoria” na página 24.

- (_RSE_JAVAOPTS) -Daudit.action=<shell script>

```
(_RSE_JAVAOPTS) -Daudit.action.id=<userid>
```

Saída de usuário baseada em z/OS UNIX que processa logs de auditoria. Para obter informações adicionais, consulte “Criação de Log de Auditoria” na página 24.

Nota: Detalhes sobre essas e outras diretivas `rse.envvars` estão disponíveis em "rse.envvars, arquivo de configuração RSE" no *Guia de Configuração do Host* (SC23-7658).

RSE - `ssl.properties`

- `daemon_keydb_file={SAF key ring name | gskkyman key database name}`
Local do certificado do daemon RSE. Para obter informações adicionais, consulte "Comunicação Criptografada de SSL/TLS" na página 29.
- `daemon_key_label=certificate label`
Nome do certificado do daemon RSE. Para obter informações adicionais, consulte "Comunicação Criptografada de SSL/TLS" na página 29.
- `server_keystore_file={SAF key ring name | Java key store name}`
Local do certificado do servidor RSE. Para obter informações adicionais, consulte "Comunicação Criptografada de SSL/TLS" na página 29.
- `server_keystore_label=certificate label`
Nome do certificado do servidor RSE. Para obter informações adicionais, consulte "Comunicação Criptografada de SSL/TLS" na página 29.
- `server_keystore_type={JKS | JCECCKARACFKS | JCECCARACFKS}`
Tipo de armazenamento de chaves usado (armazenamento de chaves Java ou conjunto de chaves SAF). Para obter informações adicionais, consulte "Comunicação Criptografada de SSL/TLS" na página 29.

Nota: Detalhes sobre essas e outras diretivas `ssl.properties` estão disponíveis em "(Opcional) `ssl.properties`, criptografia RSE SSL" no *Guia de Configuração do Host* (SC23-7658).

RSE - `pushtoclient.properties`

- `config.enabled={true | false | SAF | LDAP}`
`reject.config.updates={true | false | SAF | LDAP}`
Controle baseado em host de arquivos de configuração do cliente do Developer for System z. Para obter informações adicionais, consulte Capítulo 7, "Considerações de Push-to-client", na página 119.
- `product.enabled={true | false | SAF | LDAP}`
`reject.product.updates={true | false | SAF | LDAP}`
Controle baseado em host de atualizações do produto do cliente do Developer for System z. Para obter informações adicionais, consulte Capítulo 7, "Considerações de Push-to-client", na página 119.

Nota: Detalhe sobre essas e outras diretivas `pushtoclient.properties` estão disponíveis em "(Opcional) `pushtoclient.properties`, Controle de Cliente Baseado em Host" no *Guia de Configuração do Host* (S517-9094).

Definições de segurança

Customize e envie o membro de amostra FEKRACF, que tem comandos RACF e z/OS UNIX de amostra para criar as definições de segurança básicas para o Developer for System z.

FEKRACF está localizado em `FEK.#CUST.JCL`, a menos que tenha especificado um local quando customizou e enviou a tarefa `FEK.SFEKSAMP(FEKSETUP)`. Consulte "Configuração de Customização" no *Guia de Configuração do Host do IBM Rational Developer for System z* para obter mais detalhes.

Consulte *RACF Command Language Reference* (SA22-7687), para obter mais informações sobre comandos RACF.

Nota:

- Para esses sites que usam CA ACF2™ for z/OS, consulte a página de produto no site de suporte CA (<https://support.ca.com>) e verifique o Developer for System z Knowledge Document, TEC492389 relacionado. Este Knowledge Document tem detalhes sobre os comandos de segurança necessários para configurar adequadamente o Developer for System z.
- Para esses sites que usam CA Top Secret® for z/OS, consulte a página de produto no site de suporte de CA (<https://support.ca.com>) e verifique o Developer for System z Knowledge Document, TEC492091 relacionado. Este Knowledge Document tem detalhes sobre os comandos de segurança necessários para configurar adequadamente o Developer for System z.

As seções a seguir descrevem as etapas necessárias, configuração opcional e possíveis alternativas.

Requisitos e Lista de Verificação

Para concluir a configuração de segurança, o administrador de segurança deve conhecer os valores que estão listados em Tabela 11. Esses valores foram definidos durante as etapas anteriores da instalação e da customização do Developer for System z.

Tabela 11. Variáveis de configuração de segurança

| Descrição | <ul style="list-style-type: none">• Valor-padrão• Onde encontrar a resposta | Valor |
|---|---|-------|
| Developer for System z qualificador de alto nível do produto | <ul style="list-style-type: none">• FEK• Instalação SMP/E | |
| Developer for System z qualificador de alto nível de customização | <ul style="list-style-type: none">• FEK.#CUST• FEK.SFEKSAMP(FEKSETUP), conforme descrito em "Configuração de Customização" no <i>Guia de Configuração do Host do IBM Rational Developer for System z</i>. | |
| dNome da Tarefa Iniciada pelo Depurador Integrado | <ul style="list-style-type: none">• DBGMR• FEK.#CUST.PROCLIB(DBGMR), conforme descrito em "Mudanças em PROCLIB" no <i>Guia de Configuração do Host do IBM Rational Developer for System z</i> | |
| Nome da tarefa iniciada do JES Job Monitor | <ul style="list-style-type: none">• JMON• FEK.#CUST.PROCLIB(JMON), conforme descrito em "Mudanças de PROCLIB" no <i>Guia de Configuração do Host do IBM Rational Developer for System z</i> | |
| Nome da tarefa iniciada do daemon RSE | <ul style="list-style-type: none">• RSED• FEK.#CUST.PROCLIB(RSED), conforme descrito em "Mudanças de PROCLIB" no <i>Guia de Configuração do Host do IBM Rational Developer for System z</i>. | |
| ID do aplicativo | <ul style="list-style-type: none">• FEKAPPL• /etc/rdz/rsed.envvars, conforme descrito em "Definindo Parâmetros Extras de Inicialização Java com _RSE_JAVAOPTS" no <i>Guia de Configuração do Host do IBM Rational Developer for System z</i> | |

A lista a seguir é uma visão geral das ações que são necessárias para concluir a configuração de segurança básica do Developer for System z. Conforme

documentado nas seções a seguir, métodos diferentes podem ser usados para preencher esses requisitos, dependendo do nível de segurança necessário. Para obter informações sobre a configuração de segurança dos serviços opcionais do Developer for System z, consulte as seções anteriores.

- “Ativar Configurações de Segurança e Classes”
- “Definir um segmento OMVS para usuários do Developer for System z” na página 47
- “Definir as Tarefas Iniciadas do Developer for System z” na página 47
- “Definir RSE como um servidor z/OS UNIX seguro” na página 48
- “Definir as Bibliotecas Controladas por Programa do MVS para RSE” na página 49
- “Definir Suporte de PassTicket para RSE” na página 50
- “Definir a Proteção do Aplicativo para RSE” na página 51
- “Defina a permissão de acesso do arquivo z/OS UNIX para RSE” na página 51
- “Definir a Segurança de Comando JES” na página 52
- “Definir acesso ao depurador integrado” na página 54
- “Definir Perfis de Conjuntos de Dados” na página 54
- “Verifique as Configurações de Segurança” na página 58

Ativar Configurações de Segurança e Classes

Developer for System z usa uma variedade de mecanismos de segurança para assegurar um ambiente de sistema host seguro e controlado para o cliente. Para fazer isto, várias classes e configurações de segurança devem estar ativas, conforme mostrado com os seguintes comandos RACF de amostra:

- Exibir configurações atuais
 - SETROPTS LIST
- Ativar classe de instalação para z/OS UNIX, perfis de certificados digitais e Depurador Integrado
 - SETROPTS GENERIC(FACILITY)
 - SETROPTS CLASSACT(FACILITY) RACLIST(FACILITY)
- Ativar definições de tarefa iniciada
 - SETROPTS GENERIC(STARTED)
 - RDEFINE STARTED ** STDATA(USER(=MEMBER) GROUP(STCGROUP) TRACE(YES))
 - SETROPTS CLASSACT(STARTED) RACLIST(STARTED)
- Ativar a segurança do console para JES Job Monitor
 - SETROPTS GENERIC(CONSOLE)
 - SETROPTS CLASSACT(CONSOLE) RACLIST(CONSOLE)
- Ativar a proteção do comando do operador para JES Job Monitor
 - SETROPTS GENERIC(OPERCMDS)
 - SETROPTS CLASSACT(OPERCMDS) RACLIST(OPERCMDS)
- Ative a permissão de acesso ao arquivo z/OS UNIX para RSE
 - o SETROPTS GENERIC(UNIXPRIV)
 - o SETROPTS CLASSACT(UNIXPRIV) RACLIST(UNIXPRIV)
- Ativar a proteção do aplicativo para RSE
 - SETROPTS GENERIC(APPL)
 - SETROPTS CLASSACT(APPL) RACLIST(APPL)
- Ativar a conexão protegida usando PassTickets para RSE

- SETROPTS GENERIC(PTKTDATA)
- SETROPTS CLASSACT(PTKTDATA) RACLIST(PTKTDATA)
- Ativar o controle de programa para garantir que apenas o código confiável possa ser carregado pelo RSE
 - RDEFINE PROGRAM ** ADDMEM('SYS1.CMDLIB'//NOPADCHK) UACC(READ)
 - SETROPTS WHEN(PROGRAM)

Nota: Não crie o perfil ** se você já tiver um perfil * na classe PROGRAM. Ele obscurece e complica o caminho da procura usado pelo software de segurança. Nesse caso, você deve mesclar as definições * existentes com a ** nova. Use o perfil **, conforme documentado em *Security Server RACF Security Administrator's Guide (SA22-7683)*.

Atenção: Alguns produtos, como o FTP, precisarão ser controlados pelo programa se "WHEN PROGRAM" estiver ativo. Teste este controle de programa antes de ativá-lo em um sistema de produção.

- (Opcional) Ative o X.509 HostIdMappings e o suporte Port Of Entry (POE) estendido
 - SETROPTS GENERIC(SERVAUTH)
 - SETROPTS CLASSACT(SERVAUTH) RACLIST(SERVAUTH)

Definir um segmento OMVS para usuários do Developer for System z

Um segmento OMVS do RACF ou equivalente que especifica um ID do usuário z/OS UNIX (UID) não zero válido, diretório inicial e comando shell deve ser definido para cada usuário do Developer for System z. Seu grupo padrão também requer um segmento OMVS com um ID de grupo.

Ao usar o Depurador Integrado, o ID do usuário sob o qual o aplicativo sendo depurado está ativo e seu grupo padrão também requer um segmento RACF OMVS válido ou equivalente.

Nos comandos de amostra do RACF a seguir, substitua os marcadores #userid, #user-identifier, #group-name e #group-identifier por valores reais:

- ```
ALTUSER #userid
OMVS(UID(#user-identifier) HOME(/u/#userid) PROGRAM(/bin/sh) NOASSIZEMAX)
```
- ALTGROUP #group-name OMVS(GID(#group-identifier))

## Definir as Tarefas Iniciadas do Developer for System z

Os comandos RACF de amostra a seguir criam as tarefas iniciadas de DBGMR, JMON e RSED, com IDs do usuário protegidos (STCDBM, STCJMON e STCRSE) e o grupo STCGROUP designado a eles. Substitua os marcadores #group-id e #user-id-\* pelos IDs de OMVS válidos.

- ```
ADDGROUP STCGROUP OMVS(AUTOGID)
DATA('GROUP WITH OMVS SEGMENT FOR STARTED TASKS')
```
- ```
ADDUSER STCDBM DFLTGRP(STCGROUP) NOPASSWORD NAME('RDZ - DEBUG MANAGER')
OMVS(AUTOUID HOME(/tmp) PROGRAM(/bin/sh))
DATA('RATIONAL DEVELOPER FOR SYSTEM Z')
```
- ```
ADDUSER STCJMON DFLTGRP(STCGROUP) NOPASSWORD NAME('RDZ - JES JOBMONITOR')
OMVS(AUTOUID HOME(/tmp) PROGRAM(/bin/sh) )
DATA('RATIONAL DEVELOPER FOR SYSTEM Z')
```
- ```
ADDUSER STCRSE DFLTGRP(STCGROUP) NOPASSWORD NAME('RDZ - RSE DAEMON')
OMVS(AUTOUID HOME(/tmp) PROGRAM(/bin/sh) ASSIZEMAX(2147483647))
DATA('RATIONAL DEVELOPER FOR SYSTEM Z')
```

- ```
RDEFINE STARTED DBGMR.* DATA('RDZ - DEBUG MANAGER')
STDATA(USER(STCDBM) GROUP(STCGROUP) TRUSTED(NO))
```
- ```
RDEFINE STARTED JMON.* DATA('RDZ - JES JOBMONITOR')
STDATA(USER(STCJMON) GROUP(STCGROUP) TRUSTED(NO))
```
- ```
RDEFINE STARTED RSED.* DATA('RDZ - RSE DAEMON')
STDATA(USER(STCRSE) GROUP(STCGROUP) TRUSTED(NO))
```
- SETROPTS RACLIST(STARTED) REFRESH

Nota:

- Assegure-se de que os IDs de usuário das tarefas iniciadas sejam protegidos especificando-se a palavra-chave NOPASSWORD.
- Assegure-se de que o servidor RSE tenha um uid OMVS exclusivo devido aos privilégios relacionados ao z/OS UNIX concedidos a esse uid.
- O daemon RSE exige um tamanho de espaço de endereço grande (2GB) para operação adequada. Configure este valor na variável ASSIZEMAX do segmento OMVS para o ID do usuário STCRSE. Configurar esse valor assegura que o daemon RSE obtenha o tamanho da região necessário, independentemente de mudanças para MAXASSIZE em SYS1.PARMLIB(BPXPRMxx).
- O RSE exige também um grande número de encadeamentos para operação adequada. Você pode definir o limite na variável THREADSMAX do segmento OMVS do ID do usuário STCRSE. Configurar o limite assegura que o RSE obtenha o limite de encadeamento necessário, independentemente de mudanças para MAXTHREADS ou MAXTHREADTASKS em SYS1.PARMLIB(BPXPRMxx). Para determinar o valor correto para o limite de encadeamento, consulte "Considerações de ajuste" no *Referência de Configuração do Host* (S517-9857).
- O ID do usuário STCJMON é outro bom candidato para configurar THREADSMAX no segmento OMVS, pois o JES Job Monitor usa um encadeamento por conexão do cliente.
- A tarefa iniciada pelo Depurador Integrado (DBGMR) é usada apenas pelo recurso do Depurador Integrado opcional.

Considere tornar o ID do usuário STCRSE restrito. Usuários com o atributo RESTRICTED não podem acessar recurso protegidos (MVS) que não estão especificamente autorizados a acessar.

```
ALTUSER STCRSE RESTRICTED
```

Para assegurar que os usuários restritos não obtenham acesso a recursos do sistema de arquivos z/OS UNIX por meio de "outras" permissões de bits, defina o perfil RESTRICTED.FILESYS.ACCESS na classe UNIXPRIV com UACC(NONE). Para obter mais informações sobre restringir IDs de usuário, consulte *Security Server RACF Security Administrator's Guide* (SA22-7683).

Atenção: Se usar IDs de usuário restritos, inclua explicitamente o acesso a um recursos usando os comandos de TSO **PERMIT** ou z/OS UNIX **setfac1**. Os recursos incluem esses recursos em que a documentação do Developer for System z usa UACC, como o perfil ** na classe PROGRAM ou em que conta com convenções comuns do z/OS UNIX, como qualquer pessoa tendo permissão de leitura e execução para bibliotecas Java. Teste o acesso antes de ativá-lo em um sistema de produção.

Definir RSE como um servidor z/OS UNIX seguro

RSE requer acesso UPDATE ao perfil BPX.SERVER para criar ou excluir o ambiente de segurança para o encadeamento do cliente. Se esse perfil não estiver definido, UID(0) será necessário para o RSE. Essa etapa é necessária para que os clientes possam se conectar.

O Depurador Integrado requer acesso UPDATE ao perfil BPX.SERVER para criar ou excluir o ambiente de segurança para o encadeamento de depuração. Se este perfil não estiver definido, o UID(0) será necessário para o ID do usuário da tarefa iniciada de STCDBM. Esta permissão é necessária apenas quando o recurso Depurador Integrado opcional é usado.

- RDEFINE FACILITY BPX.SERVER UACC(NONE)
- PERMIT BPX.SERVER CLASS(FACILITY) ACCESS(UPDATE) ID(STCRSE)
- PERMIT BPX.SERVER CLASS(FACILITY) ACCESS(UPDATE) ID(STCDBM)
- SETROPTS RACLIST(FACILITY) REFRESH

Atenção: Definir o perfil BPX.SERVER torna o z/OS UNIX um comutador completo da segurança de nível UNIX para a segurança de nível z/OS UNIX, que é mais segura. Esse comutador pode afetar outros aplicativos e operações z/OS UNIX. Teste a segurança antes de ativá-la em um sistema de produção. Para obter mais informações sobre os diferentes níveis de segurança, consulte *UNIX System Services Planning* (GA22-7800).

Definir as Bibliotecas Controladas por Programa do MVS para RSE

Servidores com autoridade para BPX.SERVER devem executar em um ambiente limpo e controlado por programa. Este requisito implica que todos os programas chamados pelo RSE também devem ser controlados por programa. Para as bibliotecas de carregamento do MVS, o controle de programa é gerenciado pelo seu software de segurança. Essa etapa é necessária para que os clientes possam se conectar.

O RSE usa o tempo de execução do sistema (SYS1.LINKLIB), Language Environment' (CEE.SCEERUN*) e a biblioteca de carregamento do ISPF' TSO/ISPF Client Gateway (ISP.SISPLOAD).

- RALTER PROGRAM ** UACC(READ) ADDMEM('SYS1.LINKLIB'//NOPADCHK)
- RALTER PROGRAM ** UACC(READ) ADDMEM('SYS1.CSSLIB'//NOPADCHK)
- RALTER PROGRAM ** UACC(READ) ADDMEM('CEE.SCEERUN'//NOPADCHK)
- RALTER PROGRAM ** UACC(READ) ADDMEM('CEE.SCEERUN2'//NOPADCHK)
- RALTER PROGRAM ** UACC(READ) ADDMEM('ISP.SISPLOAD'//NOPADCHK)
- SETROPTS WHEN(PROGRAM) REFRESH

Nota: Não utilize o perfil ** se já tiver um perfil * na classe PROGRAM. O perfil obscurece e complica o caminho da procura usado por seu software de segurança. Nesse caso, você deve mesclar as definições * existentes com a ** nova. Use o perfil **, conforme documentado em *Security Server RACF Security Administrator's Guide* (SA22-7683).

As bibliotecas de pré-requisito adicionais a seguir devem ser tornadas controladas por programa para suportar o uso de serviços opcionais. Esta lista não inclui conjuntos de dados que são específicos para um produto com o qual o Developer for System z interage, tal como o IBM File Manager.

- Alterne a biblioteca de tempo de execução do REXX, para o SCLM Developer Toolkit
 - REXX.*.SEAGALT
- Biblioteca de carregamento do sistema, para criptografia SSL
 - SYS1.SIEALNKE
- Biblioteca do Developer for System z, para Depurador Integrado
 - FEK.SFEKAUTH

Nota: As bibliotecas que são projetadas para colocação de LPA também requerem autorizações de controle de programa se forem acessadas por meio de LINKLIST ou STEPLIB. Esta publicação documenta o uso das seguintes bibliotecas LPA:

- ISPF, para TSO/ISPF Client Gateway
 - ISP.SISPLPA
- Biblioteca de tempo de execução REXX, para SCLM Developer Toolkit
 - REXX.*.SEAGLPA
- Developer for System z, para CARMA
 - FEK.SFEKLPA

Definir Suporte de PassTicket para RSE

A senha do cliente ou outro meio de identificação, como o certificado X.509 é usada somente para verificar a identidade mediante a conexão. Depois disso, os PassTickets são usados para manter a segurança do encadeamento. Essa etapa é necessária para que os clientes possam se conectar.

Os PassTickets são senhas geradas pelo sistema com um tempo de vida de aproximadamente 10 minutos. Os PassTickets gerados são baseados em uma chave secreta. Esta chave é um número de 64 bits (16 caracteres hexadecimais). Nos comandos de amostra RACF a seguir, substitua o marcador key16 por uma sequência hexadecimal de 16 caracteres fornecida pelo usuário que tenha os caracteres de 0 a 9 e A a F.

- ```
RDEFINE PTKTDATA FEKAPPL.UACC(NONE) SSIGNON(KEYMASKED(key16))
APPLDATA('NO REPLAY PROTECTION - DO NOT CHANGE')
DATA('RATIONAL DEVELOPER FOR SYSTEM Z')
```
- ```
RDEFINE PTKTDATA IRRPTAUTH.FEKAPPL.* UACC(NONE)
DATA('RATIONAL DEVELOPER FOR SYSTEM Z')
```
- ```
PERMIT IRRPTAUTH.FEKAPPL.* CLASS(PTKTDATA) ACCESS(UPDATE) ID(STCRSE)
```
- ```
SETROPTS RACLIST(PTKTDATA) REFRESH
```

O RSE suporta o uso de um ID do aplicativo que não FEKAPPL. Remova o comentário e customize a opção "APPLID=FEKAPPL" em `rsed.envvars` para ativar isso, conforme documentado em "Defining extra Java startup parameters with `_RSE_JAVAOPTS`" no *IBM Rational Developer for System z Host Configuration Guide*. As definições de classe PTKTDATA devem corresponder ao ID do aplicativo real usado pelo RSE.

Não é recomendável usar OMVSAPPL como ID do aplicativo porque ele abrirá a chave secreta para a maioria dos aplicativos do z/OS UNIX. Também não é recomendável usar o ID do aplicativo padrão MVS, que é seguido do MVS pelo ID SMF do sistema, pois isso abrirá a chave secreta para a maioria dos aplicativos MVS, incluindo tarefas em lote do usuário.

Nota:

- Se a classe PTKTDATA já estiver definida, verifique se ela está definida como uma classe genérica antes de criar os perfis listados acima. O suporte para caracteres genéricos da classe PTKTDATA é novo desde o z/OS release 1.7, com a introdução de uma interface Java para PassTickets.
- Substitua o curinga (*) da definição IRRPTAUTH.FEKAPPL.* por uma máscara de ID do usuário válida para limitar os IDs do usuário para os quais o RSE pode gerar um PassTicket.

- Dependendo das configurações do RACF, o usuário que define um perfil também poderá estar na lista de acesso do perfil. Remova esta permissão para os perfis PTKTDATA.
- O JES Job Monitor e o RSE devem ter o mesmo ID de aplicativo para permitir que o JES Job Monitor avalie os PassTickets apresentados pelo RSE. Para o JES Job Monitor, o ID do aplicativo é definido no arquivo de configuração FEJJCNGF com a diretiva APPLID.
- Se o sistema tiver um produto criptográfico instalado e disponível, você poderá criptografar a chave de aplicativo de conexão protegida para proteção adicional. Para isso, use a palavra-chave KEYENCRYPTED em vez de KEYMASKED. Para obter mais informações, consulte *Security Server RACF Security Administrator's Guide* (SA22-7683).

Atenção: O pedido de conexão do cliente falhará se os PassTickets não estiverem configurados corretamente.

Defina a permissão de acesso do arquivo z/OS UNIX para RSE

O comando do operador **MODIFY LOGS** usa o ID do usuário da tarefa iniciada do RSED para coletar logs de host e informações de configuração. E por padrão, os arquivos de log do usuário, são criados com permissões de acesso do arquivo de segurança (apenas o proprietário tem acesso). Para ser capaz de coletar arquivos de log de usuários seguros, o ID do usuário da tarefa iniciada do RSED deve ter permissão para lê-los.

O argumento OWNER do comando do operador **MODIFY LOGS** resulta no ID do usuário especificado se tornar o proprietário dos dados coletados. A fim de alterar a propriedade, ao ID do usuário da tarefa inicial do RSED deve ser permitido usar o serviço CHOWN z/OS UNIX.

- RDEFINE UNIXPRIV SUPERUSER.FILESYS UACC(NONE) DATA('OVERRIDE UNIX FILE ACCESS RESTRICTIONS')
- RDEFINE UNIXPRIV SUPERUSER.FILESYS.CHOWN UACC(NONE) DATA('OVERRIDE UNIX CHANGE OWNER RESTRICTIONS')
- PERMIT SUPERUSER.FILESYS CLASS(UNIXPRIV) ACCESS(READ) ID(STCRSE)
- PERMIT SUPERUSER.FILESYS.CHOWN CLASS(UNIXPRIV) ACCESS(READ) ID(STCRSE)
- SETROPTS RACLIST(UNIXPRIV) REFRESH

Observe que quando perfil do SUPERUSER.FILESYS.ACLOVERRIDE for definido, as permissões de acesso definidas no ACL (Lista de Controle de Acesso) têm precedência sobre as permissões concedidas por meio do SUPERUSER.FILESYS. O ID do usuário da tarefa iniciada do RSED precisará da permissão de acesso do READ para o perfil do SUPERUSER.FILESYS.ACLOVERRIDE para efetuar bypass das definições de ACL.

Definir a Proteção do Aplicativo para RSE

Durante o logon do cliente, o daemon RSE verifica se um usuário tem permissão para usar o aplicativo.

- RDEFINE APPL FEKAPPL UACC(READ) DATA('RATIONAL DEVELOPER FOR SYSTEM Z')
- SETROPTS RACLIST(APPL) REFRESH

Nota:

- Conforme descrito em mais detalhes em “Definir Suporte de PassTicket para RSE” na página 50, o RSE suporta o uso de um ID do aplicativo que não FEKAPPL. A definição de classe do APPL deve corresponder ao ID do aplicativo real usado pelo RSE.
- A solicitação de conexão do cliente é bem-sucedida se o ID do aplicativo não estiver definido na classe APPL.
- A solicitação de conexão do cliente falhará somente se o ID do aplicativo estiver definido e o usuário não tiver acesso de LEITURA ao perfil.

Definir os Arquivos Controlados por Programa do z/OS UNIX para RSE

Servidores com autoridade para BPX.SERVER devem executar em um ambiente limpo e controlado por programa. Este requisito implica que todos os programas chamados pelo RSE também devem ser controlados por programa. Para arquivos z/OS UNIX, o controle de programa é gerenciado pelo comando **extattr**. Para executar esse comando, você precisa de acesso READ para o BPX.FILEATTR.PROGCTL na classe FACILITY ou ser UID(0).

O servidor RSE usa a biblioteca compartilhada Java do RACF (/usr/lib/libIRRac*.so).

- `extattr +p /usr/lib/libIRRac*.so`

Nota:

- Desde o z/OS 1.9, /usr/lib/libIRRac*.so é instalado no modo controle de programa durante a instalação do SMP/E RACF.
- Desde o z/OS 1.10, /usr/lib/libIRRac*.so é parte do SAF, que é fornecido com z/OS base, portanto, está disponível também para clientes não RACF.
- A configuração pode ser diferente se você utilizar um produto de segurança diferente do RACF. Para obter mais informações, consulte a documentação do produto de segurança.
- A instalação de SMP/E do Developer for System z configura o bit de controle de programa para programas RSE internos.
- Utilize o comando **ls -Eog** z/OS UNIX para exibir o status atual do bit de controle do programa. O arquivo é controlado por programa se a letra **p** for exibida na segunda sequência.

```
$ ls -Eog /usr/lib/libIRRac*.so
-rwxr-xr-x  aps- 2 69632 Oct 5 2007 /usr/lib/libIRRacf.so
-rwxr-xr-x  aps- 2 69632 Oct 5 2007 /usr/lib/libIRRacf64.so
```

Definir a Segurança de Comando JES

O JES Job Monitor emite todos os comandos do operador JES solicitados por um usuário por meio de um console MCS estendido (EMCS), cujo nome é controlado com a diretiva `CONSOLE_NAME`, conforme documentado em "FEJCNFG, Arquivo de Configuração do JES Job Monitor" no *Guia de Configuração do Host do IBM Rational Developer for System z*.

A amostra a seguir de comandos RACF dá aos usuários do Developer for System z a acesso condicional a um conjunto limitado de comandos JES, que são Manter, Liberar, Cancelar e Limpar. Os usuários só terão permissão de execução se emitirem os comandos por meio do JES Job Monitor. Substitua o marcador `#console` pelo nome real do console.

- ```
RDEFINE OPERCMDS MVS.MCSOPER.#console UACC(READ)
DATA('RATIONAL DEVELOPER FOR SYSTEM Z')
```

- RDEFINE OPERCMDS JES%.\* UACC(NONE)
- PERMIT JES%.\* CLASS(OPERCMDS) ACCESS(UPDATE) WHEN(CONSOLE(JMON)) ID(\*)
- SETROPTS RACLIST(OPERCMDS) REFRESH

**Nota:**

- O uso do console é permitido se nenhum perfil MVS.MCSOPER.#console for definido.
- A classe CONSOLE deverá estar ativa para que WHEN(CONSOLE(JMON)) funcione, mas não há registro de entrada real de perfil na classe CONSOLE para consoles EMCS.
- Não substitua JMON pelo nome real do console na cláusula WHEN(CONSOLE(JMON)). A palavra-chave JMON representa o aplicativo de ponto de entrada, não o nome do console.

**Atenção:** Definir os comandos JES com o acesso universal NONE no software de segurança pode afetar outros aplicativos e operações. Teste a segurança antes de ativá-la em um sistema de produção.

A Tabela 12 e a Tabela 13 mostram os comandos do operador emitidos para JES2 e JES3 e os perfis de segurança distintos que podem ser usados para protegê-los.

*Tabela 12. Comandos do Operador do JES2 Job Monitor*

| Ações     | Comando                               | Perfil OPERCMDS                                                                     | Acesso Necessário |
|-----------|---------------------------------------|-------------------------------------------------------------------------------------|-------------------|
| Suspender | \$Hx(jobid)<br>with x = {J, S or T}   | jesname.MODIFYHOLD.BAT<br>jesname.MODIFYHOLD.STC<br>jesname.MODIFYHOLD.TSU          | UPDATE            |
| Liberar   | \$Ax(jobid)<br>with x = {J, S or T}   | jesname.MODIFYRELEASE.BAT<br>jesname.MODIFYRELEASE.STC<br>jesname.MODIFYRELEASE.TSU | UPDATE            |
| Cancelar  | \$Cx(jobid)<br>with x = {J, S or T}   | jesname.CANCEL.BAT<br>jesname.CANCEL.STC<br>jesname.CANCEL.TSU                      | UPDATE            |
| Limpar    | \$Cx(jobid),P<br>with x = {J, S or T} | jesname.CANCEL.BAT<br>jesname.CANCEL.STC<br>jesname.CANCEL.TSU                      | UPDATE            |

*Tabela 13. Comandos do Operador do JES3 Job Monitor*

| Ações     | Comando      | Perfil OPERCMDS    | Acesso Necessário |
|-----------|--------------|--------------------|-------------------|
| Suspender | *F,J=jobid,H | jesname.MODIFY.JOB | UPDATE            |
| Liberar   | *F,J=jobid,R | jesname.MODIFY.JOB | UPDATE            |
| Cancelar  | *F,J=jobid,C | jesname.MODIFY.JOB | UPDATE            |
| Limpar    | *F,J=jobid,C | jesname.MODIFY.JOB | UPDATE            |

**Nota:**

- Os comandos de operador JES Manter, Liberar, Cancelar e Limpar e o comando Mostrar JCL podem ser executados somente em arquivos de spool de propriedade do ID do usuário do cliente, a menos que LIMIT\_COMMANDS= com valor LIMITED ou NOLIMIT esteja especificado no arquivo de configuração do JES Job Monitor. Para obter informações adicionais, consulte "Ações com relação a tarefas - limitações de destino" no *Referência de Configuração do Host* (S517-9857).
- Os usuários podem procurar qualquer arquivo em spool, a menos que LIMIT\_VIEW=USERID esteja definido no arquivo de configuração do JES Job Monitor. Para obter mais informações, consulte "Acesso a arquivos de spool" em *Referência de Configuração do Host* (S517-9857).
- Mesmo se os usuários não estiverem autorizados para estes comandos do operador, eles ainda poderão enviar tarefas e ler saída de tarefa por meio do JES



Job Monitor se tiverem autoridade suficiente a possíveis perfis que protegem esses recursos, como aqueles em classes JESINPUT, JESJOBS e JESSPOOL.

Supondo que a identidade do servidor JES Job Monitor, criando um console JMON a partir de uma sessão do TSO, seja impedida por seu software de segurança. Mesmo que o console possa ser criado, o ponto de entrada é diferente; por exemplo, JES Job Monitor versus TSO. Os comandos JES emitidos deste console falharão na verificação de segurança se sua segurança estiver configurada conforme documentado nesta publicação e o usuário não tiver autoridade aos comandos JES por outros meios.

## Definir acesso ao depurador integrado

Usuários requerem acesso READ para um dos seguintes perfis AQE.AUTHDEBUG.\* listados para conseguirem usar o Integrated Debugger para depurar programas de estado de problemas. Usuários permitidos para o perfil AQE.AUTHDEBUG.AUTHPGM também são permitidos para depurar programas APF autorizados. Substitua o item temporário #apf por IDs de usuários ou nomes de grupos RACF válidos para esses usuários que são autorizados a depurar programas autorizados.

- RDEFINE FACILITY AQE.AUTHDEBUG.STDPGM UACC(NONE)
- PERMIT AQE.AUTHDEBUG.STDPGM CLASS(FACILITY) ACCESS(READ) ID(\*)
- RDEFINE FACILITY AQE.AUTHDEBUG.AUTHPGM UACC(NONE)
- PERMIT AQE.AUTHDEBUG.AUTHPGM CLASS(FACILITY) ACCESS(READ) ID(#apf)
- SETROPTS RACLIST(FACILITY) REFRESH

**Nota:** Versões do Developer for System z anteriores à versão 9.1.1 usavam outro perfil de classe FACILITY, AQE.AUTHDEBUG.WRITEBUFFER, que não está mais em uso. Ela pode ser removida se o sistema host tem somente o Developer for System z versão 9.1.1 ou superior.

## Definir Perfis de Conjuntos de Dados

O acesso READ para usuários e ALTER para programadores de sistema é suficiente para a maioria dos conjuntos de dados do Developer for System z. Substitua o marcador #sysprog por IDs de usuário válidos ou nomes de grupos do RACF. Além disso, solicite ao programador de sistema que instalou e configurou o produto, os nomes de conjunto de dados corretos. FEK é o qualificador de alto nível padrão usado durante a instalação e FEK.#CUST é o qualificador de alto nível padrão para conjuntos de dados criados durante o processo de customização.

- ADDGROUP (FEK) OWNER(IBMUSER) SUPGROUP(SYS1)  
DATA('RATIONAL DEVELOPER FOR SYSTEM Z - HLQ STUB')
- ADDSD 'FEK.\*.\*' UACC(READ)  
DATA('RATIONAL DEVELOPER FOR SYSTEM Z')
- PERMIT 'FEK.\*.\*' CLASS(DATASET) ACCESS(ALTER) ID(#sysprog)
- SETROPTS GENERIC(DATASET) REFRESH

**Nota:**

- Proteja FEK.SFEKAUTH contra atualizações, pois este conjunto de dados é autorizado pelo APF. O mesmo ocorre para FEK.SFEKLOAD e FEK.SFEKLPA que, nesse caso, esses conjuntos de dados são controlados pelo programa.
- Os comandos de amostra nesta publicação e na tarefa FEKRACF supõem que a Enhanced Generic Naming (EGN) esteja ativa. Quando o EGN estiver ativo, o



qualificador \*\* poderá ser usado para representar qualquer número de qualificadores na classe DATASET. Substitua \*\* por \* se a EGN não estiver ativa em seu sistema. Para obter mais informações sobre EGN, consulte *Security Server RACF Security Administrator's Guide* (SA22-7683).

Alguns dos componentes opcionais do Developer for System z exigem perfis adicionais do conjunto de dados de segurança. Substitua os marcadores #sysprog, #ram-developer e #cicsadmin por um ID de usuário válido ou nomes de grupos RACF:

- Se a tradução do nome abreviado/Ingo do SCLM Developer Toolkit for usada, os usuários exigirão acesso UPDATE ao mapeamento VSAM, FEK.#CUST.LSTRANS.FILE.

```

-
ADDSD 'FEK.#CUST.LSTRANS.*.*' UACC(UPDATE)
DATA('RATIONAL DEVELOPER FOR SYSTEM Z - SCLMDT')
-
PERMIT 'FEK.#CUST.LSTRANS.*.*' CLASS(DATASET) ACCESS(ALTER) ID(#sysprog)
-
SETOPTS GENERIC(DATASET) REFRESH

```

- Os desenvolvedores CARMA RAM (Repository Access Manager) exigem acesso de UPDATE ao CARMA VSAMs, FEK.#CUST.CRA\*.

```

-
ADDSD 'FEK.#CUST.CRA*.*' UACC(READ)
DATA('RATIONAL DEVELOPER FOR SYSTEM Z - CARMA')
-
PERMIT 'FEK.#CUST.CRA*.*' CLASS(DATASET) ACCESS(ALTER) ID(#sysprog)
-
PERMIT 'FEK.#CUST.CRA*.*' CLASS(DATASET) ACCESS(UPDATE) ID(#ram-developer)
-
SETOPTS GENERIC(DATASET) REFRESH

```

- Se o servidor CICS Resource Definition (CRD) do Application Deployment Manager for usado, os administradores do CICS exigirão acesso UPDATE ao VSAM do repositório CRD.

```

-
ADDSD 'FEK.#CUST.ADNREP*.*' UACC(READ)
DATA('RATIONAL DEVELOPER FOR SYSTEM Z - ADN')
-
PERMIT 'FEK.#CUST.ADNREP*.*' CLASS(DATASET) ACCESS(ALTER) ID(#sysprog)
-
PERMIT 'FEK.#CUST.ADNREP*.*' CLASS(DATASET) ACCESS(UPDATE) ID(#cicsadmin)
-
SETOPTS GENERIC(DATASET) REFRESH

```

- Se o repositório de manifesto do Application Deployment Manager estiver definido, todos os usuários do CICS Transaction Server exigirão acesso UPDATE ao VSAM do repositório de manifesto.

```

-
ADDSD 'FEK.#CUST.ADNMAN*.*' UACC(UPDATE)
DATA('RATIONAL DEVELOPER FOR SYSTEM Z - ADN')
-
PERMIT 'FEK.#CUST.ADNMAN*.*' CLASS(DATASET) ACCESS(ALTER) ID(#sysprog)
-
SETOPTS GENERIC(DATASET) REFRESH

```

Use os comandos de amostra do RACF a seguir para obter uma configuração mais segura onde o acesso READ também é controlado.

- proteção do conjunto de dados uacc(none)

```

-
ADDGROUP (FEK)
DATA('RATIONAL DEVELOPER FOR SYSTEM Z - HLQ STUB')
OWNER(IBMUSER) SUPGROUP(SYS1)*
-
ADDSD 'FEK.*.*' UACC(NONE)
DATA('RATIONAL DEVELOPER FOR SYSTEM Z')
-
ADDSD 'FEK.SFEKAUTH' UACC(NONE)
DATA('RATIONAL DEVELOPER FOR SYSTEM Z')

```

```

--
ADDSD 'FEK.SFEKLOAD' UACC(NONE)
DATA('RATIONAL DEVELOPER FOR SYSTEM Z')

--
ADDSD 'FEK.SFEKMOD' UACC(NONE)
DATA('RATIONAL DEVELOPER FOR SYSTEM Z')

--
ADDSD 'FEK.SFEKPROC' UACC(NONE)
DATA('RATIONAL DEVELOPER FOR SYSTEM Z')

--
ADDSD 'FEK.#CUST.PARMLIB' UACC(NONE)
DATA('RATIONAL DEVELOPER FOR SYSTEM Z')

--
ADDSD 'FEK.#CUST.CNTL' UACC(NONE)
DATA('RATIONAL DEVELOPER FOR SYSTEM Z')

--
ADDSD 'FEK.#CUST.SQL' UACC(NONE)
DATA('RATIONAL DEVELOPER FOR SYSTEM Z')

--
ADDSD 'FEK.#CUST.LSTRANS.*.*' UACC(NONE)
DATA('RATIONAL DEVELOPER FOR SYSTEM Z - SCLMDT')

--
ADDSD 'FEK.#CUST.CRA*.*' UACC(NONE)
DATA('RATIONAL DEVELOPER FOR SYSTEM Z - CARMA')

--
ADDSD 'FEK.#CUST.ADNREP*.*' UACC(NONE)
DATA('RATIONAL DEVELOPER FOR SYSTEM Z - ADN')

--
ADDSD 'FEK.#CUST.ADNMAN*.*' UACC(NONE)
DATA('RATIONAL DEVELOPER FOR SYSTEM Z - ADN')

```

- Permitir que o programador de sistema gerencie todas as bibliotecas

```

--
PERMIT 'FEK.*.*' CLASS(DATASET) ACCESS(ALTER) ID(#sysprog)

--
PERMIT 'FEK.SFEKAUTH' CLASS(DATASET) ACCESS(ALTER) ID(#sysprog)

--
PERMIT 'FEK.SFEKLOAD' CLASS(DATASET) ACCESS(ALTER) ID(#sysprog)

--
PERMIT 'FEK.SFEKMOD' CLASS(DATASET) ACCESS(ALTER) ID(#sysprog)

--
PERMIT 'FEK.SFEKPROC' CLASS(DATASET) ACCESS(ALTER) ID(#sysprog)

--
PERMIT 'FEK.#CUST.PARMLIB' CLASS(DATASET) ACCESS(ALTER) ID(#sysprog)

--
PERMIT 'FEK.#CUST.CNTL' CLASS(DATASET) ACCESS(ALTER) ID(#sysprog)

--
PERMIT 'FEK.#CUST.SQL' CLASS(DATASET) ACCESS(ALTER) ID(#sysprog)

--
PERMIT 'FEK.#CUST.LSTRANS.*.*' CLASS(DATASET) ACCESS(ALTER) ID(#sysprog)

--
PERMIT 'FEK.#CUST.CRA*.*' CLASS(DATASET) ACCESS(ALTER) ID(#sysprog)

--
PERMIT 'FEK.#CUST.ADNREP*.*' CLASS(DATASET) ACCESS(ALTER) ID(#sysprog)

--
PERMIT 'FEK.#CUST.ADNMAN*.*' CLASS(DATASET) ACCESS(ALTER) ID(#sysprog)

```

- Permitir que os clientes acessem as bibliotecas de carregamento e execução

```

--
PERMIT 'FEK.SFEKAUTH' CLASS(DATASET) ACCESS(READ) ID(*)

--
PERMIT 'FEK.SFEKLOAD' CLASS(DATASET) ACCESS(READ) ID(*)

--
PERMIT 'FEK.SFEKPROC' CLASS(DATASET) ACCESS(READ) ID(*)

--
PERMIT 'FEK.#CUST.CNTL' CLASS(DATASET) ACCESS(READ) ID(*)

--
PERMIT 'FEK.#CUST.SQL' CLASS(DATASET) ACCESS(READ) ID(*)

```

**Nota:** Nenhuma permissão é necessária para FEK.SFEKLPA, pois todo o código que residir em LPA é acessível por todos.

- Permitir que o Nome da Tarefa Iniciada pelo Nome da Tarefa Iniciada pelo Depurador Integrado acesse a biblioteca de carregamento.
  - PERMIT 'FEK.SFEKAUTH' CLASS(DATASET) ACCESS(READ) ID(STCDBM)
- Permitir que o JES Job Monitor acesse a biblioteca de carregamento e parâmetro
  - PERMIT 'FEK.SFEKAUTH' CLASS(DATASET) ACCESS(READ) ID(STCJMON)
  - PERMIT 'FEK.#CUST.PARMLIB' CLASS(DATASET) ACCESS(READ) ID(STCJMON)
- (Opcional) Permitir que os clientes atualizem a tradução de nome abreviado/longo do VSAM para SCLMDT
  - PERMIT 'FEK.#CUST.LSTRANS\*.\*\*\*' CLASS(DATASET) ACCESS(UPDATE) ID(\*)
- (Opcional) Permitir que os desenvolvedores RAM atualizem os CARMA VSAMs para CARMA
  - PERMIT 'FEK.#CUST.CRA\*.\*\*\*' CLASS(DATASET) ACCESS(UPDATE) ID(#ram-developer)
- (Opcional) Permitir que usuários CICS leiam o VSAM do repositório CRD para Application Deployment Manager
  - PERMIT 'FEK.#CUST.ADNREP\*.\*\*\*' CLASS(DATASET) ACCESS(READ) ID(\*)
- (Opcional) Permitir que os administradores do CICS atualizem o VSAM do repositório CRD para Application Deployment Manager
  - PERMIT 'FEK.#CUST.ADNREP\*.\*\*\*' CLASS(DATASET) ACCESS(UPDATE) ID(#cicsadmin)
- (Opcional) Permitir que os usuários do CICS atualizem o VSAM do repositório de manifesto para Application Deployment Manager
  - PERMIT 'FEK.#CUST.ADNMAN\*.\*\*\*' CLASS(DATASET) ACCESS(UPDATE) ID(\*)
- (Opcional) Permitir que o servidor CICS TS acesse a biblioteca de carregamento para bidi e Application Deployment Manager
  - PERMIT 'FEK.SFEKLOAD' CLASS(DATASET) ACCESS(READ) ID(#cicsts)
- (Opcional) Permitir que o servidor CICS TS, as regiões do IMS e as tarefas em lote do MVS acessem a biblioteca de carregamento para mensagens do IRZ.
  - PERMIT 'FEK.SFEKLMOD' CLASS(DATASET) ACCESS(READ) ID(#cicsts)
  - PERMIT 'FEK.SFEKLMOD' CLASS(DATASET) ACCESS(READ) ID(#ims)
  - PERMIT 'FEK.SFEKLMOD' CLASS(DATASET) ACCESS(READ) ID(#batch)
- Ativar perfis de segurança
  - SETROPTS GENERIC(DATASET) REFRESH

Ao controlar o acesso READ para conjuntos de dados do sistema, você deve fornecer aos servidores Developer for System z e usuários a permissão READ para os seguintes conjuntos de dados:

- CEE.SCEERUN
- CEE.SCEERUN2
- CBC.SCLBDLL
- ISP.SISPLD
- ISP.SISPLPA
- SYS1.LINKLIB
- SYS1.SIEALNKE
- SYS1.SIEAMIGE
- REXX.V1R4M0.SEAGLPA

**Nota:** Ao usar a Biblioteca Alternativa para o pacote do produto REXX, o nome da biblioteca padrão de tempo de execução do REXX será REXX.\*.SEAGALT ao invés de REXX.\*.SEAGLPA, conforme usado na amostra acima.

## Verifique as Configurações de Segurança

Use os seguintes comandos de amostra para exibir os resultados de suas customizações relacionadas à segurança.

- Configurações e classes de segurança
  - SETROPTS LIST
- Segmento OMVS para usuários
  - LISTUSER #userid NORACF OMVS
  - LISTGRP #group-name NORACF OMVS
- Tarefas iniciadas
  - LISTGRP STCGROUP OMVS
  - LISTUSER STCDBM OMVS
  - LISTUSER STCJMON OMVS
  - LISTUSER STCRSE OMVS
  - RLIST STARTED DBGMR.\* ALL STDATA
  - RLIST STARTED JMON.\* ALL STDATA
  - RLIST STARTED RSED.\* ALL STDATA
- RSE como um servidor z/OS UNIX seguro
  - RLIST FACILITY BPX.SERVER ALL
- Bibliotecas controladas pelo programa MVS para RSE
  - RLIST PROGRAM \*\* ALL
- Suporte de PassTicket para RSE
  - RLIST PTKTDATA FEKAPPL ALL SSIGNON
  - RLIST PTKTDATA IRRPTAUTH.FEKAPPL.\* ALL
- Proteção do aplicativo para RSE
  - RLIST APPL FEKAPPL ALL
- A permissão de acesso ao arquivo z/OS UNIX para RSE
  - RLIST UNIXPRIV SUPERUSER.FILESYS ALL
  - RLIST UNIXPRIV SUPERUSER.FILESYS.CHOWN ALL
- Segurança do comando JES
  - RLIST CONSOLE JMON ALL
  - RLIST OPERCMDS MVS.MCSOPER.JMON ALL
  - RLIST OPERCMDS JES%.\* ALL
- Acesso integrado ao Depurador
  - RLIST FACILITY AQE.\* ALL
- Perfis do conjunto de dados
  - LISTGRP FEK
  - LISTDSD PREFIX(FEK) ALL

Opcionalmente, perfis que direcionam o comportamento do Developer for System z para um usuário específico podem existir. Esses perfis correspondem o filtro FEK.\* e são localizados por padrão na classe FACILITY. Consulte a diretiva

\_RSE\_FEK\_SAF\_CLASS em rsed.envvars. É possível usar o comando **SEARCH** para listar os nomes de perfil. Use o comando **RLIST** para mostrar os detalhes para um perfil.

- SEARCH CLASS(FACILITY) FILTER(FEK.\*\*)
- RLIST FACILITY #profile-name ALL



---

## Capítulo 3. Considerações de TCP/IP

O Developer for System z usa TCP/IP para fornecer acesso ao mainframe para usuários de uma estação de trabalho sem mainframe. Ele também usa TCP/IP para comunicação entre vários componentes e outros produtos.

Observe que a maioria das funções do Developer for System z são baseadas em z/OS UNIX e, assim, o TCP/IP usará a ordem de procura do z/OS UNIX para localizar seus arquivos de configuração. Consulte Capítulo 15, “Configurando o TCP/IP”, na página 203 para obter informações adicionais.

Os seguintes tópicos são abordados neste capítulo:

- “Portas TCP/IP”
- “Substituindo o Comportamento TCP/IP Padrão” na página 64
- “Multipilhas (CINET)” na página 64
- “Distributed Dynamic VIPA” na página 65

---

### Portas TCP/IP

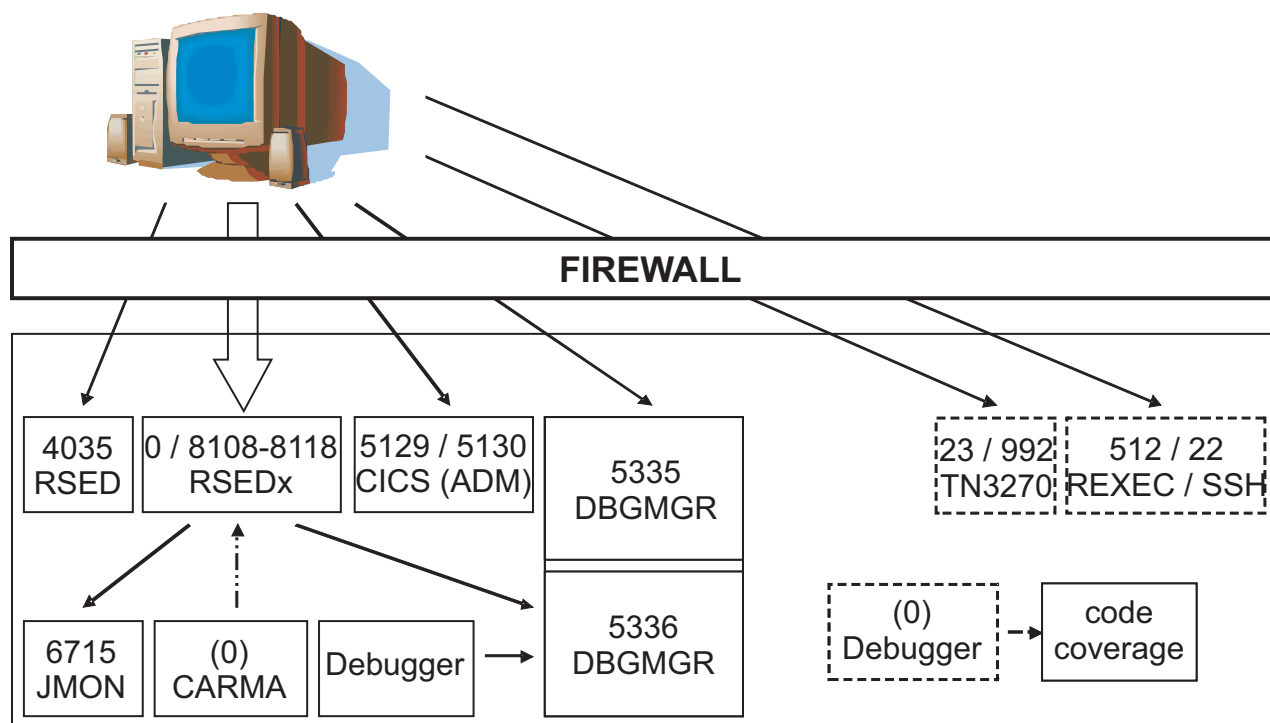


Figura 10. Portas TCP/IP

Figura 10 mostra as portas TCP/IP que podem ser usadas pelo Developer for System z. As setas mostram qual parte não liga (lado de ponta da seta) e qual se conecta.



## Comunicação Externa

Defina as seguintes portas para seu firewall protegendo o host do z/OS, uma vez que são usadas para a comunicação de cliente-host (utilizando o protocolo tcp):

- Daemon RSE para a configuração da comunicação do cliente-host, porta padrão 4035. A porta pode ser configurada no arquivo de configuração `rsed.envvars`. A comunicação nesta porta pode ser criptografada usando SSL ou TLS.
- Servidor RSE para comunicação de host do cliente. Por padrão, qualquer porta disponível é utilizada, mas isso pode ser limitado a um intervalo especificado com a definição `_RSE_PORTRANGE` no `rsed.envvars`. O intervalo de portas para `_RSE_PORTRANGE` é 8108-8118 (11 portas). A comunicação nesta porta pode ser criptografada usando SSL ou TLS.
- (opcional) Gerenciador de Depuração para serviços do Depurador Integrado, porta padrão 5335. A porta pode ser configurada no JCL de tarefa iniciada por DBGMGR. A comunicação nesta porta pode ser criptografada usando SSL ou TLS.
- (opcional) Serviço INETD para ações remotas (baseadas em host) em subprojetos z/OS UNIX:
  - REXEC (versão z/OS UNIX), porta padrão 512.
  - SSH (versão z/OS UNIX), porta padrão 22. A comunicação nessa porta é criptografada utilizando SSL.
- (opcional) Serviço Telnet TN3270 para o Emulador de Conexão do Host, porta padrão 23. A comunicação pode ser criptografada usando SSL ou TLS (porta padrão 992). A porta padrão designada ao serviço Telnet TN3270 depende de o usuário escolher ou não o uso de criptografia.
- (opcional) Uma ou as duas interfaces de aplicativo CICSTS para o Application Deployment Manager:
  - interface RESTful, porta padrão 5130. A porta pode ser configurada no CSD CICS.
  - interface de Serviços da Web, porta padrão 5129. A porta pode ser configurada no CSD CICS. A comunicação nesta porta pode ser criptografada utilizando SSL.

**Nota:** Normalmente, o cliente especifica qual endereço TCP/IP é usado para se conectar ao host. No entanto, para assegurar que as sessões de depuração se comuniquem com o host correto, o gerenciador de depuração indica ao cliente qual endereço TCP/IP deve ser usado.

## Comunicação interna

Vários serviços do host do Developer for System z executam em encadeamentos ou espaços de endereços separados e estão usando soquetes TCP/IP como mecanismo de comunicação, usando os endereços de loopback de seu sistema. Todos esses serviços usam o RSE para comunicação com o cliente, tornando seu fluxo de dados confinado apenas ao host. Para alguns serviços, será usada qualquer porta disponível, para outros, o programador de sistema poderá escolher a porta ou o intervalo de portas que será usado:

- JES Job Monitor para serviços relacionados ao JES, porta padrão 6715. A porta pode ser configurada no membro de configuração `FEJJCNFG` e é repetida no arquivo de configuração `rsed.envvars`.
- (opcional) A comunicação CARMA usa por padrão uma porta efêmera, mas um intervalo de portas pode ser configurado no arquivo de configuração `CRASRV.properties`.

- (opcional) Gerenciador de Depuração para serviços relacionados à depuração, porta padrão 5336. A porta pode ser configurada no JCL de tarefa iniciada por DBGMR.
- A cobertura de código baseado em host, que é uma tarefa em lote, aloca uma porta efêmera para permitir que o IBM Debug Tool for z/OS se comunique com ela e entregue os dados necessários para o relatório de cobertura de código.

## Reserva de Porta TCP/IP

Se usar a instrução PORT ou PORTRANGE em PROFILE.TCPIP para reservar as portas usadas pelo Developer for System z, observe que muitas ligações são feitas por encadeamentos ativos em um conjunto de encadeamentos RSE. O nome da tarefa do conjunto de encadeamentos do RSE é RSEDx, em que RSED é o nome da tarefa iniciada do RSE e x é um número aleatório de um dígito; assim, curingas são obrigatórios na definição.

```
PORT 4035 TCP RSED ; Developer para System z - RSE daemon
PORT 6715 TCP JMON ; Developer para System z - JES job monitor
PORT 5335 TCP DBGMR ; Developer for System z - Integrated
debugger
PORT 5336 TCP DBGMR ; Developer for System z - Integrated
debugger
PORTRange 8108 11 TCP RSED* ; Developer para System z - _RSE_PORTRANGE
;PORTRange 5227 100 TCP RSED* ; Developer para System z - CARMA
```

## portas do CARMA e TCP/IP

O CARMA (Common Access Repository Manager) é usado para acessar um host baseado em Software Configuration Manager (SCM), por exemplo, o CA Endevor® SCM. Na maioria dos casos, como no daemon RSE, um servidor se conecta a uma porta e atende a pedidos de conexão. O CARMA, no entanto, usa uma abordagem diferente, uma vez que o servidor CARMA não está ativo ainda quando o cliente inicia o pedido de conexão.

Quando o cliente envia uma solicitação de conexão, o minerador CARMA, que está ativo como um encadeamento de usuários em um conjunto de encadeamentos RSE, solicitará uma porta efêmera ou localizará uma porta livre no intervalo especificado no arquivo de configuração CRASRV.properties e ligará a ele. O extrator inicia então o servidor CARMA e transmite o número da porta, para que o servidor saiba a que porta se conectar. Quando o servidor estiver conectado, o cliente poderá enviar solicitações ao servidor e receber os resultados.

A partir de uma perspectiva TCP/IP, o RSE (por meio do minerador CARMA) é o servidor que liga a porta e o servidor CARMA é o cliente que se conecta a ela.

Se usar a instrução PORT ou PORTRANGE em PROFILE.TCPIP para reservar o intervalo de porta usado pelo CARMA, observe que o minerador CARMA está ativo em um conjunto de encadeamentos RSE. O nome da tarefa do conjunto de encadeamentos do RSE é RSEDx, em que RSED é o nome da tarefa iniciada RSE e x é um número aleatório de um dígito, assim são necessários caracteres curinga na definição.

```
PORTRange 5227 100 RSED* ; Developer para System z - CARMA
```

**Nota:** O CARMA IVP, fekfivpc, falhará se as portas do CARMA forem reservadas para uso pelos espaços de endereço do RSE. Isto é para ser esperado por que o IVP executa no espaço de endereço da pessoa que está executando o IVP, e não no espaço de endereço do RSE, e o TCP/IP falhará a solicitação de ligação.

## Considerações de LDAP

O servidor RSE pode ser configurado para consultar um ou mais servidores LDAP para vários serviços do Developer for System z:

- Consultar grupos LDAP para obter suporte push-to-client a vários grupos de desenvolvedores.
- Consultar uma ou mais Listas de Revogação de Certificado (CRLs) para autenticação X.509.

Observe que medidas de segurança de TCP/IP, como firewalls, podem fazer com que o servidor RSE (baseado em host) pare de entrar em contato com o servidor LDAP. Use as informações a seguir para assegurar que o servidor LDAP possa ser atingido:

- Os endereços TCP/IP ou nomes DNS do servidor LDAP são listados nas variáveis \*\_LDAP\_SERVER em `rsed.envvars`.
- Os números de porta do servidor LDAP são listados nas variáveis \*\_LDAP\_PORT em `rsed.envvars`.
- O LDAP usa o protocolo TCP.
- O servidor LDAP é contatado pelo servidor RSE baseado em host.
- O servidor RSE está ativo em um espaço de endereço RSEDx, em que RSED é o nome da tarefa iniciada do RSE e x é um número aleatório de um dígito, por exemplo, RSED8.

---

## Substituindo o Comportamento TCP/IP Padrão

### ACK Atrasado

O ACK atrasado atrasa o reconhecimento (ACK) do recebimento de um pacote TCP em até 200 ms. Esse atraso aumenta a chance de que o ACK possa ser enviado com a resposta ao pacote recebido, reduzindo o tráfego de rede. Entretanto, se o remetente ficar aguardando o ACK antes de enviar um novo pacote (por exemplo, devido à implementação do algoritmo de Nagle) e não houver resposta ao pacote que acabou de ser enviado (por exemplo, porque ele faz parte de uma transferência de arquivo), a comunicação é atrasada desnecessariamente.

O Developer for System z permite que você desative a função de ACK atrasado. No host, isso é feito com a diretiva `DSTORE_TCP_NO_DELAY` em `rsed.envvars`, conforme documentado no *Guia de Configuração do Host* (S517-9094).

---

## Multipilhas (CINET)

O z/OS Communication Server permite que você tenha diversas pilhas TCP/IP simultaneamente ativas em um único sistema. Isso é chamado configuração CINET.

Se Developer for System z não estiver ativo na pilha padrão, as funções selecionadas do Developer for System z podem falhar. A afinidade de pilha é um modo seguro para resolver isso. Ela instrui o Developer for System z a usar apenas determinada pilha TCP/IP (em vez de cada pilha TCP/IP disponível, que é o padrão para tarefas iniciadas).

A afinidade de pilha está configurada para a tarefa de RSED iniciada removendo o comentário e customizando a diretiva `_BPXK_SETIBMOPT_TRANSPORT` no arquivo de configuração `rsed.envvars`. Consulte a seção relacionada no "Capítulo 2 Customização Básica" do *Guia de Configuração do Host* (SC23-7658) para obter mais detalhes sobre como customizar este arquivo de configuração.

## O CARMA e a Afinidade de Pilha

O CARMA (Common Access Repository Manager) é usado para acessar um host baseado em Software Configuration Manager (SCM), por exemplo, o CA Endevor® SCM. Para fazer isso, o CARMA inicia um servidor específico do usuário, que necessita de configuração adicional para impor a afinidade de pilha.

Semelhante às tarefas iniciadas do Developer for System z, a afinidade de pilha de um servidor CARMA é configurada com a variável `_BPXK_SETIBMOPT_TRANSPORT`, que deve ser passada para o LE (Language Environment). Isso pode ser feito ajustando o comando de inicialização no arquivo de configuração `crastart*.conf` ou `CRASUB*`.

### Nota:

- O nome exato do arquivo de configuração que contém o comando de inicialização depende das várias opções feitas pelo programador de sistemas que configurou o CARMA. Consulte o "Capítulo 3. (Opcional) Common Access Repository Manager (CARMA)" no *Guia de Configuração do Host(S517-9094)* para obter mais informações sobre isso.
- `_BPXK_SETIBMOPT_TRANSPORT` especifica o nome da pilha TCP/IP a ser usada, como definido na instrução `TCPIPJOBNAME` no `TCPIP.DATA` relacionado.
- Codificar uma instrução `SYSTCPD DD` não configura a afinidade de pilha solicitada.
- Por padrão, o CARMA não usa as pilhas de TCP/IP normais. O CARMA usa o endereço de loopback para comunicação entre o minerador CARMA e o servidor CARMA. Isso melhora a segurança (apenas os processos locais possuem acesso ao endereço de loopback) e pode evitar a necessidade de incluir afinidade de pilha na comunicação do CARMA.

### **crastart\*.conf**

Substitua esta parte:

```
... PARM(&CRAPRM1. &CRAPRM2.)
```

por esta (em que `TCPIP` representa a pilha TCP/IP desejada):

```
... PARM(ENVAR("_BPXK_SETIBMOPT_TRANSPORT=TCPIP") / &CRAPRM1. &CRAPRM2.)
```

**Nota:** `CRASUB*` não suporta continuações de linha, mas não há nenhum limite quanto ao comprimento de linha aceito.

### **CRASUB\***

Substitua esta parte:

```
... PARM(&PORT &TIMEOUT)
```

por esta (em que `TCPIP` representa a pilha TCP/IP desejada):

```
... PARM(ENVAR("_BPXK_SETIBMOPT_TRANSPORT=TCPIP") / &PORT &TIMEOUT)
```

**Nota:** O envio da tarefa limita o comprimento de linha em 80 caracteres. É possível quebrar uma linha mais longa em um espaço em branco ( ) e usar um sinal de mais (+) no final da primeira linha para concatenar as 2 linhas.

---

## Distributed Dynamic VIPA

O DVIPA (Dynamic Virtual IP Addressing) distribuído permite que você execute simultaneamente configurações Developer for System z idênticas em diferentes sistemas em seu sysplex e faça com que o TCP/IP, opcionalmente com a ajuda de WLM, distribua as conexões do cliente entre esses sistemas.

Há várias maneiras de se configurar um DVIPA distribuído, mas o Developer for System z impõe algumas restrições nessas opções.

- O daemon RSE possui a porta que é definida para o DVIPA distribuído, mas o trabalho real ocorre no servidor RSE, o qual está ativado como um encadeamento em outro espaço de endereço. Portanto, você não pode usar o método de distribuição SERVERWLM para fazer o balanceamento de carga entre seus sistemas, porque o WLM irá aconselhar com base nas estatísticas do daemon RSE, não no servidor RSE.
- O cliente conhece apenas o endereço DVIPA usado pelo Sysplex Distributor para daemon RSE. O Sysplex Distributor passará o pedido de conexão para um dos daemons RSE disponíveis, que por sua vez iniciará um encadeamento do servidor RSE que se conectará a uma porta nesse sistema. Quando o cliente se conectar a esta porta, ele usará o endereço DVIPA novamente e não o endereço real do sistema, portanto, você deve assegurar-se de que o Sysplex Distributor redirecione a nova conexão para o sistema correto.

Portanto, o Developer for System z requer a definição de SYSPLEXPORTS na instrução VIPADISTRIBUTE para assegurar que as portas usadas pelos encadeamentos do servidor RSE sejam exclusivas no sysplex.

**Nota:**

- O uso de SYSPLEXPORTS significa que a estrutura EZBEPORTRANGE deve ser definida em seu recurso de acoplamento.
- O uso de SYSPLEXPORTS implica em que o TCP/IP irá selecionar uma porta efêmera para a conexão secundária. Isso quer dizer que você não pode reservar portas para essas conexões em seu perfil TCP/IP com as diretivas PORT e PORTRANGE. Também não é possível usar \_RSE\_PORTRANGE em rsed.envvars para limitar as portas usadas pelo Developer for System z. O Developer for System z não fornece uma solução alternativa para essa restrição, porque isso complica a configuração do firewall.

Existem também algumas restrições no Developer for System z ao usar DVIPA distribuído:

- A diretiva enable.dDVIPA em rsed.envvars deve estar ativa.
- Para assegurar que o cliente Developer for System z não irá interferir na seleção da porta correta pelo TCP/IP, é necessário habilitar a diretiva deny.nonzero.port em rsed.envvars.
- Todos os servidores Developer for System z participantes devem ter uma configuração idêntica. Você deve compartilhar /usr/lpp/rdz e /etc/rdz entre todos os sistemas participantes. Compartilhe também /var/rdz/projects, /var/rdz/pushtoclient e /var/rdz/scldmt, se esses diretórios estiverem em uso. Observe que /var/rdz/WORKAREA e /var/rdz/logs devem ser exclusivos para cada sistema.
- Consulte Capítulo 11, “Executando várias instâncias”, na página 157 para saber quais componentes do Developer for System z devem ser compartilhados e quais devem ser exclusivos por sistema.

JES Job Monitor, CARMA e outros servidores do Developer for System z somente interagem com o RSE local e, portanto, não requerem uma configuração DVIPA.

O Depurador Integrado interage com o RSE local e, portanto, não requer uma configuração de DVIPA. Para assegurar que as sessões de depuração se comuniquem com o host correto, o gerenciador de depuração informa ao cliente qual endereço TCP/IP deve ser usado e, dessa forma, não requer uma configuração de DVIPA.

Os DVIPAs distribuídos são definidos pelas palavras-chave VIPADefine e VIPABackup do bloco VIPADynamic em seu perfil TCP/IP. A palavra-chave VIPADISTribute inclui as definições necessárias do Sysplex Distributor. O DVIPA distribuído requer que todas as pilhas participantes estejam de acordo com o sysplex, o que é feito por meio das palavras-chave SYSPLExRouting e DYNAMICXCF do bloco IPCONFIG em seu perfil TCP/IP. Consulte *Communications Server: IP Configuration Reference* (SC31-8776) para obter detalhes adicionais sobre essas diretivas.

Consulte *MVS Setting Up a Sysplex* (SA22-7625) e *Communication Server: SNA Network Implementation Guide* (SC31-8777) para obter mais informações sobre a configuração da estrutura EZBEPORPTS em seu recurso de acoplamento.

## Restringindo a Seleção de Portas

O uso de SYSPLExPORTS implica em que o TCP/IP irá selecionar uma porta efêmera para a conexão secundária. Uma porta efêmera é qualquer porta que esteja livre e não reservada de nenhuma forma. O uso de uma porta efêmera conflita com a melhor prática de firewall de limitar as portas que estão abertas para comunicação, porque não se sabe qual porta será usada.

É possível contornar esse problema forçando o Developer for System z a usar portas conhecidas para a conexão secundária definindo um \_RSE\_PORTRANGE exclusivo por sistema e assegurando que os intervalos de portas usados sejam reservados para uso do Developer for System z em todos os sistemas. Observe que essa solução requer o APAR de TCP/IP PM63379.

Para assegurar que o TCP/IP irá rotear a conexão secundária para o sistema correto, o Developer for System z deve usar um intervalo de portas exclusivo em cada sistema. Isso implica em que não é possível usar uma configuração idêntica compartilhada para os sistemas, pois \_RSE\_PORTRANGE em rsed.envvars deve ser exclusivo. Consulte “Arquivos de Configuração Diferentes de Níveis de Software Idênticos” na página 158 em Capítulo 11, “Executando várias instâncias”, na página 157 para obter informações sobre como configurar diversos servidores com diferentes arquivos de configuração usando o mesmo código. Você deve usar uma cópia principal de rsed.envvars e um script para ajustar e copiar em uma configuração específica ao sistema para assegurar que o arquivo permaneça idêntico em diferentes sistemas.

1. Configure Developer for System z em SYS1 como se fosse uma configuração de um único sistema, mas assegure-se de que /usr/lpp/rdz e /etc/rdz estejam localizados em um sistema de arquivos compartilhado. Todas as partes baseadas em MVS também devem ser compartilhadas com SYS2.
2. Use /etc/rdz/rsed.envvars como a cópia principal e inclua uma referência para /etc/rdz no final do arquivo, de modo que as cópias específicas dos sistemas possam apanhar os arquivos de configuração restantes.

```
$ oedit /etc/rdz/rsed.envvars
-> add the following at the END:
-- NEEDED TO FIND THE REMAINING CONFIGURATION FILES
CFG_BASE=/etc/rdz
CLASSPATH=.:$CFG_BASE:$CLASSPATH
--
```

3. Crie /etc/rdz/update.sh, um shell script que irá copiar o rsed.envvars principal e ajustar \_RSE\_PORTRANGE

```
$ oedit /etc/rdz/update.sh
$ chmod 755 /etc/rdz/update.sh
```



```

#!/bin/sh
Materiais Licenciados - Propriedade da IBM
5724-T07 Copyright IBM Corp. 2012
clone rsed.envvars e configure PORTRANGE para uso com RDz & DDVIPA

file=rsed.envvars #; echo file $file
sys=${1:-$(sysvar SYSNAME)} #; echo sys $sys
dir=$(dirname $0) #; echo dir $dir
se sysname tiver um caractere especial, preceda-o com \ (ex. SYS\1)
case "$sys" in
 "SYS1") range=8108-8118;;
 "SYS2") range=8119-8129;;
 *) # #### CUSTOMIZE ESTA SEÇÃO ####
esac
esac #; echo range $range
echo "configurando o intervalo de portas $range para $sys usando $dir/$file"

if test ! $range ; then
 echo ERROR: nenhum intervalo de portas definido para $sys ; exit 12 ; fi
if test ! -e $dir/$file ; then
 echo ERROR: o arquivo $dir/$file não existe ; exit 12 ; fi
if test ! -d $dir/$sys ; then
 echo ERROR: o diretório $dir/$sys não existe ; exit 12 ; fi

mv $dir/$sys/$file $dir/$sys/prev.$file 2>/dev/null
sed="/_RSE_PORTRANGE/s/./_RSE_PORTRANGE=$range/"
sed "$sed" $dir/$file > $dir/$sys/$file

if test ! -s $dir/$sys/$file ; then
 echo ERRO ao criar $dir/$sys/$file, restaurando o backup
 mv $dir/$sys/prev.$file $dir/$sys/$file ; exit 8 ; fi

```

*Figura 11. update.sh - Suportar Configuração de DDVIPA com um Firewall*

4. Crie os diretórios /etc/rdz/SYS1 e /etc/rdz/SYS2 e execute /etc/rdz/update.sh para preencher os diretórios.

```

$ mkdir /etc/rdz/SYS1 /etc/rdz/SYS2
$ /etc/rdz/update.sh SYS1
configurando o intervalo de portas 8108-8118 para SYS1 usando
/etc/rdz/rsed.envvars
$ /etc/rdz/update.sh SYS2
configurando o intervalo de portas 8119-8129 para SYS2 usando
/etc/rdz/rsed.envvars

```

5. Assegure-se de que a tarefa iniciada RSED aponte para /etc/rdz/&SYSNAME.

```
// CNFG='/etc/rdz/&SYSNAME.'
```

Em seguida, você deve assegurar-se de que os intervalos de portas definidos sejam reservados para o Developer for System z em todos os sistemas no sysplex para garantir que o número da porta permaneça exclusivo dentro do sysplex. Use a instrução PORT ou PORTRANGE em PROFILE.TCPIP para reservar todos os intervalos em todos os sistemas. O nome da tarefa do conjunto de encadeamentos do RSE é RSEDx, em que RSED é o nome da tarefa iniciada do RSE e x é um número aleatório de um dígito; assim, curingas são obrigatórios na definição.

```

PORTRange 8108 22 RSED* ; 8108-8129 - Developer para System z
 ; - conexão secundária

```

Conforme documentado em “Fluxo de conexão” na página 8, o intervalo de portas em \_RSE\_PORTRANGE pode ser pequeno. O servidor RSE não precisa da porta exclusivamente pela duração da conexão do cliente. Ela só é necessária no momento da expansão entre (servidor) a ligação e (cliente) a conexão que nenhum outro servidor RSE pode se conectar à porta. Isso significa que a maioria das conexões estará usando a primeira porta no intervalo, com o restante do intervalo sendo um buffer no caso de diversos logons simultâneos.

## Configuração de Amostra

Na configuração de amostra a seguir existem dois sistemas z/OS, SYS1 e SYS2, que fazem parte de um sysplex. O System SYS1 é definido como o sistema que normalmente hospeda o Sysplex Distributor para o DVIPA distribuído Developer for System z.

Depois de definir o DVIPA distribuído, o Developer for System z pode ser iniciado nos sistemas para permitir as conexões do cliente do balanceamento de carga em todos os sistemas. O JES Job Monitor apenas interage com o RSE local e, portanto, não requer uma configuração DVIPA. Os clientes se conectarão à porta 4035 no



endereço IP 10.10.10.1.

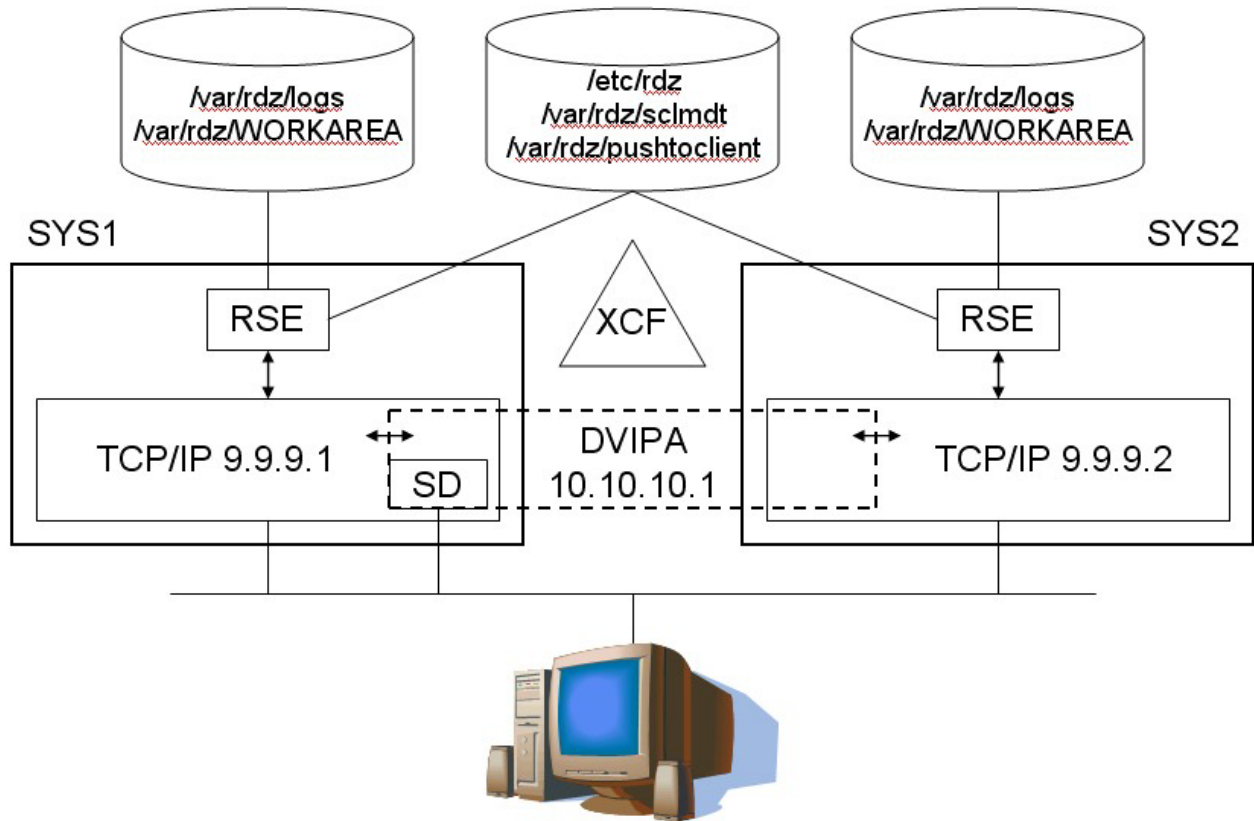


Figura 12. Amostra do Distributed Dynamic VIPA

### Sistema SYS1 – Perfil TCP/IP

```
IPCONFIG
 SYSPLEXRouting
; SYSPLEXROUTING é necessário, pois esta pilha precisa da comunicação sysplex
 DYNAMICXCF 9.9.9.1 255.255.255.0 1
; DYNAMICXCF define o dispositivo/link com o endereço home 9.9.9.1 conforme necessário
 IGNORERedirect

VIPADYNAMIC
 VIPADefine 255.255.255.0 10.10.10.1
; VIPADefine define 10.10.10.1 como DVIPA principal no SYS1 para RDz
 VIPADISTRIBUTE DEFINE
; VIPADISTRIBUTE torna 10.10.10.1 um DVIPA distribuído, deve corresponder ao SYS2
 SYSPLEXPORTS ; RDz prereq
 DISTMETHOD BASEWLM ; BASEWLM or ROUNDROBIN
 10.10.10.1 ; endereço DVIPA usado por clientes RDz
 PORT 4035 ; porta usada por clientes RDz
 DESTIP 9.9.9.1 9.9.9.2 ; RDz ativo em SYS1 e SYS2
ENDVIPADYNAMIC
```

### Sistema SYS2 – Perfil TCP/IP

```
IPCONFIG
 SYSPLEXRouting
; SYSPLEXROUTING é necessário, pois esta pilha precisa da comunicação sysplex
 DYNAMICXCF 9.9.9.2 255.255.255.0 1
; DYNAMICXCF define o dispositivo/link com o endereço home 9.9.9.2 conforme necessário
 IGNORERedirect

VIPADYNAMIC
 VIPABACKUP 255.255.255.0 10.10.10.1
; VIPABACKUP define 10.10.10.1 como um DVIPA de backp em SYS2 para RDz
 VIPADISTRIBUTE DEFINE
; VIPADISTRIBUTE torna 10.10.10.1 um DVIPA distribuído, deve corresponder a SYS1
 SYSPLEXPORTS ; RDz prereq
 DISTMETHOD BASEWLM ; BASEWLM or ROUNDROBIN
 10.10.10.1 ; endereço DVIPA usado por clientes RDz
 PORT 4035 ; porta usada por clientes RDz
 DESTIP 9.9.9.1 9.9.9.2 ; RDz ativo em SYS1 e SYS2
ENDVIPADYNAMIC
```



---

## Capítulo 4. Considerações WLM

Ao contrário dos aplicativos tradicionais do z/OS, o Developer for System z não é um aplicativo monolítico que pode ser identificado facilmente para Workload Manager (WLM). O Developer for System z consiste de vários componentes que interagem para fornecer ao cliente acesso para os serviços e dados do host. Como descrito em Capítulo 1, “Entendendo o Developer for System z”, na página 3, alguns destes serviços estão ativos em espaços de endereços diferentes, resultando em classificações WLM diferentes.

Os seguintes tópicos são abordados neste capítulo:

- “Classificação de Carga de Trabalho”
- “Configurando Objetivos” na página 73

---

### Classificação de Carga de Trabalho

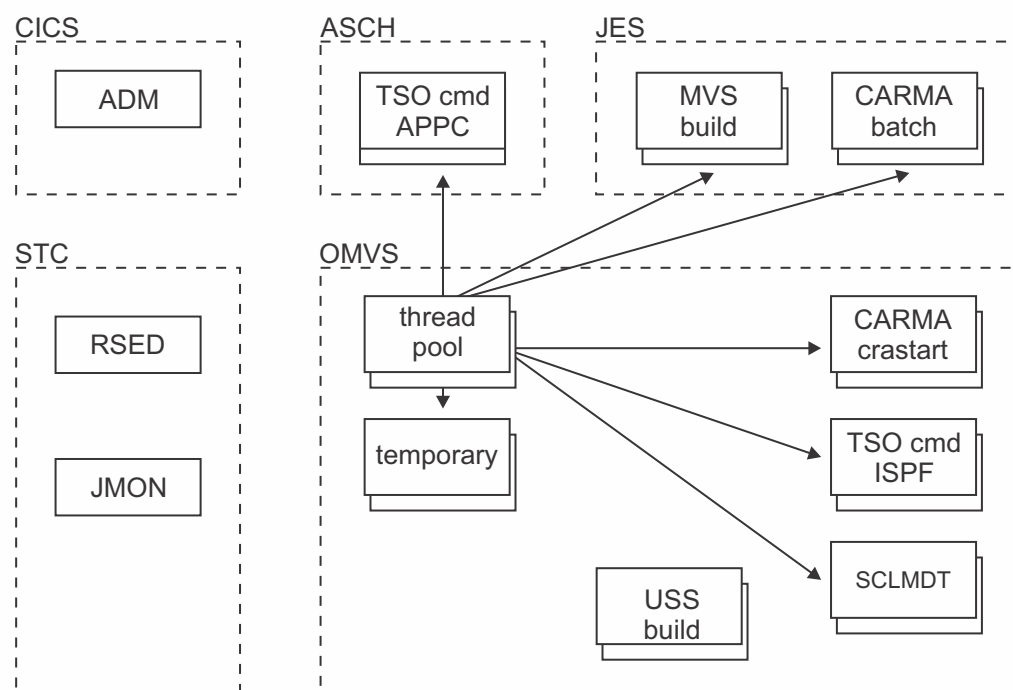


Figura 13. classificação WLM

O Figura 13 mostra uma visão geral básica dos subsistemas por meio dos quais as cargas de trabalho do Developer for System z são apresentadas ao WLM.

O Application Deployment Manager (ADM) está ativo dentro de uma região CICS e, portanto, seguirá as regras de classificação do CICS no WLM.

O RSE daemon (RSED), Debug Manager (DBGMGR) e o JES Job Monitor (JMON) são tarefas iniciadas do Developer for System z (ou tarefas em lote de longa execução), cada uma com seu espaço de endereço individual.

Como documentado em “RSE como um aplicativo Java” na página 5, o daemon RSE gera um processo-filho para cada servidor de conjunto de encadeamentos RSE (que suporta um número variável de clientes). Cada conjunto de encadeamentos está ativo em um espaço de endereço separado (usando um iniciador z/OS UNIX, BPXAS). Porque estes são processos gerados, eles são classificados usando as regras de classificação WLM OMVS, e não as regras de classificação de tarefa iniciada.

Os clientes que estão ativos em um conjunto de encadeamentos podem criar uma infinidade de outros espaços de endereços, dependendo das ações realizadas pelos usuários. Dependendo da configuração de Developer for System z algumas cargas de trabalho, como o serviço TSO Commands (TSO cmd) ou CARMA, podem executar em subsistemas diferentes.

Os espaços de endereços listados em Figura 13 na página 71 permanecem no sistema o tempo suficiente para serem visíveis, mas você deve estar ciente que devido à maneira como o z/OS UNIX é projetado, há também vários espaços de endereços temporários de curta duração. Estes espaços de endereços temporários estão ativos nos subsistemas OMVS.

Note que enquanto os conjuntos de encadeamento RSE usam o mesmo ID do usuário e um nome de tarefa similar como o daemon RSE, todos os espaços de endereços iniciados por um conjunto de encadeamento são de propriedade do ID do usuário do cliente solicitando a ação. O ID de usuário cliente também é usado como (parte de) o nome da tarefa para todos os espaços de endereço baseados em OMVS iniciados pelo conjunto de encadeamentos.

Mais espaços de endereços são criados por outros serviços que o Developer for System z usa, como o File Manager (FMNCAS) ou o z/OS UNIX REXEC (construção USS).

## Regras de Classificação

O WLM usa regras de classificações para mapear o trabalho entrando no sistema para uma classe de serviço. Esta classificação é baseada nos qualificadores de trabalho. O primeiro qualificador (obrigatório) é um tipo de subsistema que recebe o pedido de trabalho. O Tabela 14 lista os tipos de subsistema que podem receber cargas de trabalho Developer for System z.

*Tabela 14. Subsistemas de Ponto de Entrada do WLM*

| Tipos de subsistemas | Descrição do trabalho                                                                                                                                       |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ASCH                 | Os pedidos de trabalho incluem todos os programas de transação APPC planejados pelo planejador de transação da IBM-supplied APPC/MVS, ASCH.                 |
| CICS                 | Os pedidos de trabalho incluem todas as transações processadas pelo CICS.                                                                                   |
| JES                  | Os pedidos de trabalho incluem todos os trabalhos que o JES2 ou JES3 iniciam.                                                                               |
| OMVS                 | Os pedidos de trabalho incluem o trabalho processado nos espaços de endereços filhos bifurcados no z/OS UNIX System Services.                               |
| STC                  | Os pedidos de trabalho incluem todo o trabalho iniciado pelos comandos START e MOUNT. O STC também inclui os espaços de endereços do componente do sistema. |

A Tabela 15 lista qualificadores adicionais que podem ser usados para designar uma carga de trabalho a uma classe de serviço específica. Consulte MVS Planejamento: Gerenciamento de Carga de Trabalho (SA22-7602) para obter detalhes adicionais sobre os qualificadores de trabalho listados.

*Tabela 15. Qualificadores de trabalho WLM*

|    |                | ASCH | CICS | JES | OMVS | STC |
|----|----------------|------|------|-----|------|-----|
| AI | Dados da Conta | x    |      | x   | x    | x   |

**Tabela 15. qualificadores de trabalho WLM (continuação)**

|     |                                  | ASCH | CICS | JES | OMVS | STC |
|-----|----------------------------------|------|------|-----|------|-----|
| LU  | Nome LU (*)                      |      | x    |     |      |     |
| PF  | Perform (*)                      |      |      | x   |      | x   |
| PRI | Prioridade                       |      |      | x   |      |     |
| SE  | Nome de Ambiente de Planejamento |      |      | x   |      |     |
| SSC | Nome de Coleta de Subsistema     |      |      | x   |      |     |
| SI  | Instância de Subsistema (*)      |      | x    | x   |      |     |
| SPM | Parâmetro de Subsistema          |      |      |     |      | x   |
| PX  | Nome Sysplex                     | x    | x    | x   | x    | x   |
| SY  | Nome do Sistema (*)              | x    |      |     | x    | x   |
| TC  | Transação/Classe de Trabalho (*) | x    |      | x   |      |     |
| TN  | Transação/Nome do Trabalho (*)   | x    | x    | x   | x    | x   |
| UI  | ID do usuário (*)                | x    | x    | x   | x    | x   |

**Nota:** Para os qualificadores marcados com (\*), é possível especificar os grupos de classificação ao incluir um G na abreviação do tipo. Por exemplo, um grupo de nome de transação seria TNG.

## Configurando Objetivos

Como documentado em “Classificação de Carga de Trabalho” na página 71, o Developer for System z cria tipos diferentes de cargas de trabalho no seu sistema. Estas diferentes tarefas comunicam-se entre si, o que implica que o tempo decorrido real tornar-se importante para evitar problemas de tempo limite para as conexões entre as tarefas. Como resultado, Developer for System z é recomendável que as tarefas sejam colocadas em classes de serviço de alto desempenho ou em classes de serviço de desempenho moderado com uma alta prioridade.

Uma revisão, e possivelmente uma atualização, dos seus objetivos WLM atuais é, por essa razão, aconselhado. Isto é especialmente verdadeiro para empresas tradicionais MVS novas no que diz respeito às cargas de trabalho OMVS de tempo crítico.

### Nota:

- As informações sobre os objetivos nesta seção são deliberadamente mantidas em um nível descritivo porque os objetivos de desempenho reais são muito específicos do site.
- Para ajudar no entendimento do impacto de uma tarefa específica no seu sistema, termos como recursos substanciais, moderados e mínimos são usados. Todos eles são relativos ao uso total de recurso Developer for System z, ele mesmo, mas não de todo o sistema.

O Tabela 16 lista os espaços de endereços que são usados pelo Developer for System z. O z/OS UNIX substituirá "x" na coluna "Nome da Tarefa" por um número de 1 dígito aleatório.

**Tabela 16. cargas de trabalho WLM**

| Descrição                                                 | Nome da tarefa | Carga de trabalho |
|-----------------------------------------------------------|----------------|-------------------|
| Debug Manager                                             | DBGMGR         | STC               |
| JES Job Monitor                                           | JMON           | STC               |
| Daemon RSE                                                | RSED           | STC               |
| Conjunto de encadeamento do RSE                           | RSEDx          | OMVS              |
| ISPF Client Gateway (Serviço do TSO Commands e do SCLMDT) | <userid>x      | OMVS              |
| Serviço do TSO Commands (APPC)                            | FEKFRSRV       | ASCH              |
| CARMA (batch)                                             | CRA<port>      | JES               |

Tabela 16. cargas de trabalho WLM (continuação)

| Descrição                                  | Nome da tarefa       | Carga de trabalho |
|--------------------------------------------|----------------------|-------------------|
| CARMA (crastart)                           | <userid>x            | OMVS              |
| CARMA (ISPF Client Gateway)                | <userid> e <userid>x | OMVS              |
| Build MVS (tarefa em lote)                 | *                    | JES               |
| Build z/OS UNIX (comandos do shell)        | <userid>x            | OMVS              |
| Shell do z/OS UNIX                         | <userid>             | OMVS              |
| Gerenciador de Implementação de Aplicativo | CICSTS               | CICS              |

## Considerações para Seleção de Objetivos

As seguintes considerações gerais do WLM podem ajudar a definir apropriadamente as definições de objetivos corretas para Developer for System z:

- É recomendável que você baseie os objetivos no que é realmente possível ser atingido e não no que você deseja que aconteça. Se estabelecer objetivos mais altos do que o necessário, o WLM moverá recursos de trabalho de importância menor para trabalho de importância mais alta, que pode não necessariamente precisar de recursos.
- Limite a quantia de trabalho designada para classes de serviços SYSTEM e SYSSTC porque essas classes possuem uma prioridade de despacho mais alta que qualquer classe WLM gerenciada. Use estas classes para trabalho que seja de importância alta, mas que use pouco CPU.
- O trabalho que é desaprovado pelas regras de classificação acaba na classe SYSOTHER, que possui um objetivo discricionário. Um objetivo discricionário diz ao WLM para apenas fazer o seu melhor, quando o sistema possuir recursos sobressalentes.

Quando usar os objetivos de tempo de resposta:

- Deve haver uma taxa de chegada de tarefas fixa (pelo menos 10 tarefas em 20 minutos) para que o WLM gerencie apropriadamente um objetivo de tempo de resposta.
- Use objetivos de tempo médio de resposta somente para cargas de trabalho bem controladas, porque uma única transação longa possui um grande impacto sobre o tempo médio de resposta e pode fazer com que o WLM reaja exageradamente.

Quando usar objetivos de velocidade:

- Normalmente, não é possível atingir uma meta de velocidade acima de 90% por várias razões. Por exemplo, todos os espaços de endereços SYSTEM e SYSSTC possuem uma prioridade de despacho mais alto que o objetivo de tipo de velocidade.
- O WLM usa um número mínimo de (uso e atraso) amostras nas quais baseia suas decisões sobre objetivo de velocidade. Assim quando menor for a execução de trabalho em uma classe de serviço, maior será o tempo para coletar o número requerido de amostras e ajustar a política de despacho.
- Reavalie os objetivos de velocidade quando alterar o seu hardware. Em particular, mover para processadores mais rápidos e menores requer mudanças nos objetivos de velocidade.

## STC

Todas as tarefas iniciadas do Developer for System z, daemons RSE e JES Job Monitor, estão atendendo solicitações de cliente em tempo real.

*Tabela 17. cargas de trabalho WLM STC*

| Descrição       | Nome da tarefa | Carga de trabalho |
|-----------------|----------------|-------------------|
| JES Job Monitor | JMON           | STC               |
| Debug Manager   | DBGMGR         | STC               |
| Daemon RSE      | RSED           | STC               |

- JES Job Monitor

O JES Job Monitor fornece todos os serviços relacionados a JES, como enviar tarefas, navegar arquivos de spool e executar comandos de operador JES. É recomendável especificar um objetivo de velocidade de um período, e com alta prioridade, porque a tarefa não relata transações individuais para o WLM. O uso de recurso depende fortemente das ações do usuário e, por essa razão, vai variar, mas é esperado que seja de mínimo a moderado.

- Debug Manager

O Debug Manager fornece serviços para conectar programas que estão sendo depurados para clientes que os estão depurando. É recomendável especificar um objetivo de velocidade de um período, e com alta prioridade, porque a tarefa não relata transações individuais para o WLM. O uso de recursos depende fortemente das ações do usuário, e, por essa razão, vai variar, mas é esperado ser o mínimo.

- Daemon RSE

O daemon RSE trata da criação do logon e autenticação do cliente e gerencia os diferentes conjuntos de encadeamentos RSE. É recomendável especificar um objetivo de velocidade de um período, e com alta prioridade, porque a tarefa não relata transações individuais para o WLM. Espera-se ser mínimo o uso de recurso, com um pico no começo do dia útil.

## OMVS

As cargas de trabalho OMVS podem ser divididas em dois grupos, conjuntos de encadeamentos RSE e todo o resto. Isto porque todas as cargas de trabalho, exceto os conjuntos de encadeamentos RSE, usam o ID de usuário cliente como base para o nome do espaço de endereço. (O z/OS UNIX substituirá "x" na coluna "Nome da Tarefa" por um número de 1 dígito aleatório.

*Tabela 18. Cargas de trabalho WLM OMVS*

| Descrição                                                 | Nome da tarefa       | Carga de trabalho |
|-----------------------------------------------------------|----------------------|-------------------|
| Conjunto de encadeamento do RSE                           | RSEDx                | OMVS              |
| ISPF Client Gateway (Serviço do TSO Commands e do SCLMDT) | <userid>x            | OMVS              |
| CARMA (crastart)                                          | <userid>x            | OMVS              |
| CARMA (ISPF Client Gateway)                               | <userid> e <userid>x | OMVS              |
| Build z/OS UNIX (comandos do shell)                       | <userid>x            | OMVS              |
| Shell do z/OS UNIX                                        | <userid>             | OMVS              |

- Conjunto de encadeamento do RSE

Um conjunto de encadeamentos RSE é como o coração e o cérebro do Developer for System z. Quase todos os dados circulam por aqui e os mineradores (encadeamentos específicos do usuário) dentro do conjunto de encadeamentos controlam as ações da maioria das outras tarefas relacionadas do Developer for System z. É recomendável especificar um objetivo de velocidade de um período, e com alta prioridade, porque a tarefa não relata transações individuais para o WLM. O uso de recursos depende fortemente das ações do usuário e, por essa razão, vai variar, mas é esperado ser substancial.

Todas as cargas de trabalho restantes terminarão na mesma classe de serviço devido a uma convenção de nomenclatura do espaço de endereço comum. É



recomendável especificar um objetivo de período múltiplo para esta classe de serviço. Os primeiros períodos deveriam ser de objetivos de tempo de resposta percentil e de alto desempenho, enquanto que o último período deveria possuir um objetivo de velocidade de desempenho moderado. Algumas cargas de trabalho, como a ISPF Client Gateway, relatarão transações individuais para o WLM, enquanto outras não.

- ISPF Client Gateway

O ISPF Client Gateway é um serviço ISPF invocado pelo Developer for System z para executar comandos TSO e ISPF não interativos. Isto inclui os comandos explícitos emitidos pelo cliente e também os comandos implícitos emitidos pelo Developer for System z, como obter uma lista de membros PDS. O uso de recursos depende fortemente das ações do usuário, e, por essa razão, vai variar, mas é esperado ser o mínimo.

- CARMA

O CARMA é um servidor Developer for System z opcional usado para interagir com Software Configuration Managers (SCMs), baseados em host, tais como o CA Endevor® SCM. O Developer for System z permite diferentes métodos de inicialização para um servidor CARMA, alguns dos quais transformam-se em uma carga de trabalho OMVS. O uso de recursos depende fortemente das ações do usuário, e, por essa razão, vai variar, mas é esperado ser o mínimo.

- Build z/OS UNIX

Quando um cliente inicia uma construção para um projeto z/OS UNIX, o z/OS UNIX REXEC (ou SSH) iniciará uma tarefa que executa um número de comandos shell do z/OS UNIX para executar a construção. O uso dos recursos depende fortemente das ações do usuário e, por essa razão, vai variar, mas é esperado ser de moderado a substancial, dependendo do tamanho do projeto.

- Shell do z/OS UNIX

Esta carga de trabalho processa os comandos shell do z/OS UNIX que são emitidos pelo cliente. O uso de recursos depende fortemente das ações do usuário, e, por essa razão, vai variar, mas é esperado ser o mínimo.

## JES

Os processos em lote do JES gerenciado são usados de várias maneiras pelo Developer for System z. O uso mais comum é para construções MVS, onde uma tarefa é submetida e monitorada para determinar quando ela termina. Mas o Developer for System z também poderia iniciar um servidor CARMA em lote e comunicar-se com ele usando TCP/IP.

*Tabela 19. Carga de trabalhos WLM JES*

| Descrição                  | Nome da tarefa | Carga de trabalho |
|----------------------------|----------------|-------------------|
| CARMA (batch)              | CRA<port>      | JES               |
| Build MVS (tarefa em lote) | *              | JES               |

- CARMA

O CARMA é um servidor Developer for System z opcional usado para interagir com Software Configuration Managers (SCMs), baseados em host, tais como o CA Endevor® SCM. O Developer for System z permite diferentes métodos de inicialização para um servidor CARMA, alguns dos quais transformam-se em uma carga de trabalho JES. É recomendável especificar um objetivo de velocidade de um período, e com alta prioridade, porque a tarefa não relata transações individuais para o WLM. O uso de recursos depende fortemente das ações do usuário, e, por essa razão, vai variar, mas é esperado ser o mínimo.

- Build MVS

Quando o cliente inicia uma construção para um projeto MVS, Developer for System z iniciará um trabalho em lote para executar a construção. O uso dos recursos depende fortemente das ações do usuário e, por essa razão, vai variar, mas é esperado ser de moderado a substancial, dependendo do tamanho do projeto. Estratégias diferentes de objetivos de desempenho moderado é aconselhável, dependendo das circunstâncias locais.

- Você poderia especificar um objetivo de período múltiplo com um período de tempo de resposta percentil e um período de velocidade de final. Neste caso, seus desenvolvedores deveriam estar usando principalmente o mesmo procedimento de construção e arquivos de entrada de tamanho similar para criar tarefas com tempos de resposta uniformes. Também deve haver uma taxa de chegada de tarefas fixa (pelo menos 10 tarefas em 20 minutos) para que o WLM gerencie apropriadamente o objetivo de tempo de resposta.
- Um objetivo de velocidade é mais adequado para a maioria de tarefas em lote porque este objetivo pode lidar com taxas de chegada e tempos de execução altamente variáveis.

## ASCH

Nas versões atuais do Developer for System z, o ISPF Client Gateway é usado para executar comandos TSO e ISPF não interativos. Devido a razões históricas, o Developer for System z também suporta executar estes comandos por meio de uma transação APPC. Você deve observar que o método APPC é reprovado.

*Tabela 20. Cargas de trabalho WLM ASCH*

| Descrição                      | Nome da tarefa | Carga de trabalho |
|--------------------------------|----------------|-------------------|
| Serviço do TSO Commands (APPC) | FEKFRSRV       | ASCH              |

- serviço TSO Commands

O serviço TSO Commands pode ser iniciado como uma transação APPC pelo Developer for System z para executar os comandos TSO e ISPF não interativos. Isto inclui os comandos explícitos emitidos pelo cliente e também os comandos implícitos emitidos pelo Developer for System z, como obter uma lista de membros PDS. É recomendável especificar um objetivo de período múltiplo para esta classe de serviço. Para os primeiros períodos, é recomendável especificar objetivos de tempo de resposta percentil e de alto desempenho. Para o período final, é recomendável especificar um objetivo de velocidade de desempenho moderada. O uso de recursos depende fortemente das ações do usuário, e, por essa razão, vai variar, mas é esperado ser o mínimo.

## CICS

O Application Deployment Manager é um servidor Developer for System z opcional que está ativo dentro de uma região do CICS Transaction Server.

*Tabela 21. Cargas de trabalho WLM - CICS*

| Descrição                                  | Nome da tarefa | Carga de trabalho |
|--------------------------------------------|----------------|-------------------|
| Gerenciador de Implementação de Aplicativo | CICSTS         | CICS              |

- Gerenciador de Implementação de Aplicativo

O servidor opcional do Application Deployment Manager, que é ativo dentro de uma região CICSTS, permite que você transfira com segurança tarefas de gerenciamento CICSTS selecionadas para desenvolvedores. O uso de recursos depende fortemente das ações do usuário, e, por essa razão, vai variar, mas é esperado ser o mínimo. O tipo de classe de serviço a ser usado depende das outras transações ativas nesta região CICS e, portanto, não é discutido em detalhes.

O WLM suporta vários tipos de gerenciamento que você pode usar para CICS:

- Gerenciando o CICS através de um objetivo de região

O objetivo é configurado para uma classe de serviço que gerencia os espaços de endereços CICS. Só é possível usar um objetivo de velocidade de execução para esta classe de serviço. O WLM usa as regras de classificação JES ou STC para os espaços de endereços, mas não usa as regras de classificação do subsistema CICS para transações.

- Gerenciando o CICS através de um objetivo de tempo de resposta de transação

O objetivo de tempo de resposta pode ser configurado em uma classe de serviço designada para uma única transação ou um grupo de transações. O WLM usa as regras de classificação JES ou STC para os espaços de endereços e as regras de classificação do subsistema CICS para transações.

---

## Capítulo 5. Considerações de Ajuste

Conforme explicado em Capítulo 1, “Entendendo o Developer for System z”, na página 3, o RSE (Explorador de Sistema Remoto) é o núcleo do Developer for System z. Para gerenciar as conexões e as cargas de trabalho a partir dos clientes, o RSE é formado por um espaço de endereço do daemon, que controla os espaços de endereços do conjunto de encadeamento. O daemon age como um ponto focal para fins de conexão e gerenciamento, enquanto os conjuntos de encadeamentos processam as cargas de trabalho do cliente.

Isso torna o RSE um alvo principal para o ajuste da configuração do Developer for System z. Entretanto, manter centenas de usuários, cada um usando 17 ou mais encadeamentos, uma certa quantia de armazenamento, e possivelmente 1 ou mais espaços de endereços requer uma configuração adequada de ambos Developer for System z e z/OS.

Os seguintes tópicos são abordados neste capítulo:

- “Uso de Recursos”
- “Uso de Armazenamento” na página 93
- “Uso do espaço do sistema de arquivos z/OS UNIX” na página 98
- “Definições de Recursos Principais” na página 100
- “Várias definições de recurso” na página 104
- “Monitoramento” na página 106
- “Configuração de Amostra” na página 109

---

### Uso de Recursos

Use as informações nesta seção para estimar o uso normal e máximo de recursos pelo Developer for System z, para que possa planejar sua configuração do sistema de acordo.

Ao usar os números e as fórmula apresentados nesta seção para definir os valores dos limites do sistema, lembre-se de que você está trabalhando com estimativas bastante precisas. Deixe margem suficiente ao configurar os limites do sistema para permitir o uso de recursos por tarefas temporárias e outras tarefas, ou por usuários que se conectam várias vezes ao host simultaneamente. (Por exemplo, por meio de RSE e de TN3270).

#### Nota:

- As informações são limitadas ao escopo para serviços acessados por meio do RSE que são fornecidas pelo próprio Developer for System z. Por exemplo, o uso de recurso do TN3270 não é documentado (não acessado por meio do RSE), nem o uso de recursos dos programas chamados durante construções remotas (baseadas em host) dos projetos MVS ou z/OS UNIX (não fornecido pelo Developer for System z).
- Incluir extensões de terceiros no Developer for System z pode aumentar os contadores de uso de recurso.
- Todos os serviços têm tarefas de “manutenção” de curta duração, que usam recursos durante sua execução, e que podem ser executados em sequência ou em paralelo entre si. Os recursos usados por essas tarefas não são documentados.

- Onde for útil, o uso de recursos específicos do usuário de software obrigatório, como o ISPF Client Gateway, é documentado.
- Os números apresentados aqui podem ser alterados sem notificação prévia.

## Visão Geral (Overview)

As tabelas a seguir dão uma visão geral do número de espaços de endereços, processos e encadeamentos usados pelo Developer for System z. Mais detalhes sobre os números apresentados aqui podem ser localizados nas seções de texto:

- “Contagem do espaço de endereço” na página 81
- “Contagem de processos” na página 83
- “Contagem de encadeamentos” na página 86

Tabela 22 dá uma visão geral dos principais recursos usados pelas tarefas iniciadas do Developer for System z. Esses recursos são alocados apenas uma vez. Eles são compartilhados entre clientes do Developer for System z.

*Tabela 22. Uso de recursos comuns*

| Tarefa iniciada | Espaços de endereço | Processos | Encadeamentos |
|-----------------|---------------------|-----------|---------------|
| JMON            | 1                   | 1         | 3             |
| DBGMR           | 1                   | 1         | 4             |
| RSED            | 1                   | 3         | 16            |
| RSEDx           | (a) 1 + 2           | 1 + 3     | 1 + 14        |

**Nota:** (a) Existe um espaço de endereço autorizado pelo APF e pelo menos um conjunto de encadeamentos RSE, o que consiste em dois espaços de endereço. Consulte “Contagem do espaço de endereço” na página 81 para determinar o número real de espaços de endereços do conjunto de encadeamento do RSE.

A Tabela 23 fornece uma visão geral dos recursos principais usados pelo software obrigatório. Esses recursos são alocados para cada cliente do Developer for System z que chama a função relacionada.

*Tabela 23. Uso de recursos obrigatórios específicos do usuário*

| Software obrigatório | Espaços de endereço | Processos | Encadeamentos |
|----------------------|---------------------|-----------|---------------|
| ISPF Client Gateway  | 1                   | 2         | 4             |
| APPC                 | 1                   | 1         | 2             |

Tabela 24 dá uma visão geral dos principais recursos por cada cliente do Developer for System z ao executar a função especificada. Valores não numéricos, como ISPF, são uma referência ao valor correspondente na Tabela 23.

*Tabela 24. Uso de recursos específicos do usuário*

| Ação do usuário                      | Espaços de endereço | Processos     | Encadeamentos |       |      |
|--------------------------------------|---------------------|---------------|---------------|-------|------|
|                                      | ID do usuário       | ID do usuário | ID do usuário | RSEDx | JMON |
| Logon                                | -                   | -             | -             | 17    | 1    |
| Cronômetro para tempo limite inativo | -                   | -             | -             | 1     | -    |
| Procurar                             | -                   | -             | -             | 1     | -    |
| Expandir PDS(E)                      | ISPF                | ISPF          | ISPF          | -     | -    |
| Abrir conjunto de dados              | ISPF                | ISPF          | ISPF          | 1     | -    |
| Comando TSO                          | ISPF                | ISPF          | ISPF          | -     | -    |
| Shell do z/OS UNIX                   | 1                   | 1             | 1             | 6     | -    |
| Build MVS                            | 1                   | -             | -             | -     | -    |
| Build z/OS UNIX                      | 3                   | 3             | 3             | -     | -    |

Tabela 24. Uso de recursos específicos do usuário (continuação)

| Ação do usuário              | Espaços de endereço | Processos     | Encadeamentos |       |      |
|------------------------------|---------------------|---------------|---------------|-------|------|
|                              | ID do usuário       | ID do usuário | ID do usuário | RSEDx | JMON |
| CARMA (batch)                | 1                   | 1             | 2             | 1     | -    |
| CARMA (crastart)             | 1                   | 1             | 2             | 1     | -    |
| CARMA (crastart com rastreo) | 3                   | 1+1+2         | 1+1+1+2       | 2     | -    |
| CARMA (ispf)                 | 4                   | 4             | 7             | 5     | -    |
| SCLMDT                       | ISPF                | ISPF          | ISPF          | -     | -    |

**Nota:** O ISPF pode ser substituído pelo APPC, exceto para o SCLM Developer Toolkit.

## Contagem do espaço de endereço

Tabela 25 lista os espaços de endereços que são usados pelo Developer for System z, em que “u” na coluna “Count” indica que a quantia deve ser multiplicada pelo número de usuários ativos simultaneamente usando a função. O z/OS UNIX substituirá “x” na coluna “Nome da Tarefa” por um número de 1 dígito aleatório.

Tabela 25. Contagem do espaço de endereço

| Contador | Descrição                                                 | Nome da tarefa              | Compartilhado | Termina após                            |
|----------|-----------------------------------------------------------|-----------------------------|---------------|-----------------------------------------|
| 1        | JES Job Monitor                                           | JMON                        | Sim           | Nunca                                   |
| 1        | Debug Manager                                             | DBGMGR                      | Sim           | Nunca                                   |
| 1        | Daemon RSE                                                | RSED                        | Sim           | Nunca                                   |
| 1        | RSE daemon APF autorizado                                 | RSEDx                       | Sim           | Nunca                                   |
| (a)      | Conjunto de encadeamento do RSE                           | RSEDx                       | Sim           | Nunca                                   |
| (a)      | APF do conjunto de encadeamentos do RSE autorizado        | RSEDx                       | Sim           | Nunca                                   |
| 1u       | ISPF Client Gateway (Serviço do TSO Commands e do SCLMDT) | <userid>x                   | Não           | 15 minutos ou no logoff do usuário      |
| 1u       | Serviço do TSO Commands (APPC)                            | FEKFRSRV                    | Não           | 60 minutos ou efetuar logoff do usuário |
| 1u       | CARMA (batch)                                             | CRA<port>                   | Não           | 7 minutos ou no logoff do usuário       |
| 1u       | CARMA (crastart)                                          | <userid>x                   | Não           | 7 minutos ou no logoff do usuário       |
| 3u       | CARMA (crastart com rastreo) (c)                          | <userid> e <userid>x        | Não           | 7 minutos ou no logoff do usuário       |
| 4u       | CARMA (ispf, descontinuado)                               | (1)<userid> ou (3)<userid>x | Não           | 7 minutos ou no logoff do usuário       |
| (b)      | Uso simultâneo do ISPF Client Gateway por 1 usuário       | <userid>x                   | Não           | Conclusão da tarefa                     |
| 1u       | Build MVS (tarefa em lote)                                | *                           | Não           | Conclusão da tarefa                     |
| 3u       | Build z/OS UNIX (comandos do shell)                       | <userid>x                   | Não           | Conclusão da tarefa                     |
| 1u       | Shell do z/OS UNIX                                        | <userid>                    | Não           | Logoff do usuário                       |

### Nota:

- (a) Existe pelo menos um espaço de endereço do conjunto de encadeamento do RSE ativo. O número real depende de:
  - A diretiva `minimum.threadpool.process` em `rsed.envvars`. O valor-padrão é 1.
  - O número de usuários que podem ser atendidos por um conjunto de encadeamento. As configurações padrão são planejadas para 30 usuários por conjunto de encadeamentos.

**Nota:** Se a diretiva `single.logon` estiver ativa, haverá pelo menos 2 conjuntos de encadeamento iniciados, mesmo que `minimum.threadpool.process` esteja configurado como 1. A configuração padrão para `single.logon` em `rsed.envvars` está ativa.

- (b) Developer for System z tem diversos encadeamentos ativos por usuário. No caso de o espaço de endereço do ISPF Client Gateway não tiver terminado de atender aos pedido de um encadeamento quando outro encadeamento enviar

um pedido, o ISPF inicializará um novo Client Gateway para processar o novo pedido. Esse espaço de endereço termina após a conclusão da tarefa.

- (c) rastreamento de inicialização crastart do CARMA é controlado pelo nível de depuração de RSE ativo para o rsecomm.log.
- O SCLMDT exige um espaço de endereço do ISPF Client Gateway. O SCLMDT compartilha o espaço de endereço com o serviço do TSO Commands.
- A maioria das ações relacionadas ao conjunto de dados do MVS usa o serviço do TSO Commands, que pode estar ativo no ISPF Client Gateway ou em uma transação do APPC, respectivamente.

Use a fórmula em Figura 14 para estimar o número máximo de espaços de endereços usados pelo Developer for System z.

$$3 + 2 * A + N * (x + y + z) + (2 + N * 0.01)$$

Figura 14. Número máximo de espaços de endereço

Em que,

- “3” é igual ao número de espaços de endereço do servidor ativo permanente.
- “A” representa o número de espaços de endereço de conjunto de encadeamentos do RSE.
- “N” representa o número máximo de usuários simultâneos.
- “x” é um dos seguintes valores, dependendo das opções de configuração selecionadas.

| X | SCLMDT | TSO por meio do Client Gateway | TSO por meio do APPC |
|---|--------|--------------------------------|----------------------|
| 1 | Não    | Não                            | Sim                  |
| 1 | Não    | Sim                            | Não                  |
| 1 | Sim    | Sim                            | Não                  |

- “y” é um dos seguintes valores, dependendo das opções de configuração selecionadas.

| S |                                   |
|---|-----------------------------------|
| 0 | Sem CARMA                         |
| 1 | CARMA (batch)                     |
| 1 | CARMA (crastart)                  |
| 3 | CARMA (crastart com rastreamento) |
| 4 | CARMA (ispf, descontinuado)       |

- “z” é 0 por padrão, mas pode aumentar dependendo das ações do usuário:
  - Inclua 1 quando um build MVS for executado. Esses espaços de endereço terminam quando a tarefa do build relacionado (uma tarefa em lote) for concluída.
  - Inclua 3 quando um build z/OS UNIX for executado. Observe que o número real pode ser alto, dependendo das necessidades dos programas invocados. Esses espaços de endereço terminam quando a tarefa do build relacionada for concluída.
- “2 + N\*0.01” inclui um buffer para espaços de endereço temporários. O tamanho do buffer necessário pode ser diferente no seu site.

Use a fórmula em Figura 15 na página 83 para estimar o número máximo de espaços de endereços usados por um cliente Developer for System z (não contando



os espaços de endereços temporários não documentados).

$$x + y + z$$

Figura 15. Número de espaços de endereços por cliente

Em que,

- "x" depende das opções de configuração selecionadas e é documentado na fórmula para calcular o número máximo de espaços de endereço (Figura 14 na página 82).
- "y" depende das opções de configuração selecionadas e é documentado na fórmula para calcular o número máximo de espaços de endereço (Figura 14 na página 82).
- "z" é 0 por padrão, mas pode aumentar, dependendo das ações do usuário, conforme documentado na fórmula para calcular o número máximo de espaços de endereço (Figura 14 na página 82).

As definições na Tabela 26 podem limitar o número real de espaços de endereço.

Tabela 26. Limites de espaço de endereço

| Local        | Limite                     | Recursos afetados                                                      |
|--------------|----------------------------|------------------------------------------------------------------------|
| rsed.envvars | maximum.threadpool.process | Limita o número de conjuntos de encadeamento do RSE                    |
| IEASYMxx     | MAXUSER                    | Limita o número de espaços de endereço                                 |
| ASCHPMxx     | MAX                        | Limita o número de iniciadores APPC para o serviço TSO Commands (APPC) |

## Contagem de processos

Tabela 27 lista o número de processos por espaço de endereço que é usado pelo Developer for System z. "u" na coluna "Address Spaces" indica que a quantia deve ser multiplicada pelo número de usuários ativos simultaneamente usando a função.

Tabela 27. Contagem de processos

| Processos | Espaços de endereço | Descrição                                                 | ID do usuário |
|-----------|---------------------|-----------------------------------------------------------|---------------|
| 1         | 1                   | JES Job Monitor                                           | STCJMON       |
| 1         | 1                   | Debug Manager                                             | STCDBM        |
| 3         | 1                   | Daemon RSE                                                | STCRSE        |
| 1         | 1                   | RSE daemon autorizado pelo APF                            | STCRSE        |
| 2         | (a)                 | Conjunto de encadeamento do RSE                           | STCRSE        |
| 1         | (a)                 | Conjunto de encadeamento RSE autorizado pelo APF          | STCRSE        |
| 2         | (b)                 | ISPF Client Gateway (Serviço do TSO Commands e do SCLMDT) | <userid>      |
| 2         | (a)                 | Conjunto de encadeamento do RSE                           | STCRSE        |
| 1         | 1u                  | Serviço do TSO Commands (APPC)                            | <userid>      |
| 1         | 1u                  | CARMA (batch)                                             | <userid>      |
| 1         | 1u                  | CARMA (crastart)                                          | <userid>      |
| 1+1+2     | 3u                  | CARMA (crastart com rastreo) (c)                          | <userid>      |
| 1         | 1u                  | CARMA (ispf, descontinuado)                               | <userid>      |
| 1         | 3u                  | Build z/OS UNIX (comandos do shell)                       | <userid>      |
| 1         | 1u                  | Shell do z/OS UNIX                                        | <userid>      |
| (5)       | (u)                 | SCLM Developer Toolkit                                    | <userid>      |

**Nota:**

- (a) Existe pelo menos 1 espaço de endereço do conjunto de encadeamento do RSE ativo. Consulte “Contagem do espaço de endereço” na página 81 para determinar o número real de espaços de endereços do conjunto de encadeamento do RSE.
- O daemon RSE e todos os conjuntos de encadeamento do RSE usam o mesmo ID de usuário.
- (b) Em situações normais e ao usar as opções de configuração padrão, existe 1 ISPF Client Gateway ativo por usuário. O número real pode variar, conforme descrito em “Contagem do espaço de endereço” na página 81.
- (c) rastreamento de inicialização do CARMA CRAFT é controlado pelo nível de depuração de RSE ativo para o rsecomm.log.
- O SCLMDT exige um espaço de endereço do ISPF Client Gateway. O SCLMDT compartilha o espaço de endereço com o serviço do TSO Commands.
- (u) Os processos SCLMDT são executados no espaço de endereço do ISPF Client Gateway e, portanto, não possuem um valor para a contagem do espaço de endereço.
- Os processos SCLMDT são temporários e terminam na conclusão da tarefa, mas vários processos podem estar ativos simultaneamente para um único usuário. A Tabela 27 na página 83 lista o número máximo de processos SCLMDT simultâneos.
- A maioria das ações relacionadas ao conjunto de dados do MVS usa o serviço do TSO Commands, que pode estar ativo no ISPF Client Gateway ou em uma transação do APPC, respectivamente.
- Um build z/OS UNIX usa três processos no total, cada um executando em seu próprio espaço de endereço.
- Todos os processos listados permanecem ativos até que o espaço de endereço relacionado termine, a menos que indicado de outra forma.

Use a fórmula em Figura 16 para estimar o número máximo de processos usados pelo Developer for System z.

$$6 + 3 * A + N * (x + y + z) + (10 + N * 0.05)$$

Figura 16. Número máximo de processos

Em que,

- “6” equivale ao número de processos usados pelos espaços de endereço do servidor ativo permanente.
- “A” representa o número de espaços de endereço de conjunto de encadeamentos do RSE.
- “N” representa o número máximo de usuários simultâneos.
- “x” é um dos seguintes valores, dependendo das opções de configuração selecionadas.

| X | SCLMDT | TSO por meio do Client Gateway | TSO por meio do APPC |
|---|--------|--------------------------------|----------------------|
| 1 | Não    | Não                            | Sim                  |
| 2 | Não    | Sim                            | Não                  |
| 7 | Sim    | Sim                            | Não                  |

- “y” é um dos seguintes valores, dependendo das opções de configuração selecionadas.

| S |                               |
|---|-------------------------------|
| 0 | Sem CARMA                     |
| 1 | CARMA (batch)                 |
| 1 | CARMA (crastart)              |
| 4 | CARMA (crastart com rastreio) |
| 4 | CARMA (ispf, descontinuado)   |

- "z" é 0 por padrão, mas pode aumentar dependendo das ações do usuário:
  - Inclua 1 quando um shell z/OS UNIX for aberto. Esse processo permanece ativo até que o usuário efetue logoff.
  - Inclua 3 quando um build z/OS UNIX for executado. Observe que o número real pode ser alto, dependendo das necessidades dos programas invocados. Esses processos terminam quando a tarefa do build relacionada for concluída.
- "10 + N\*0.05" inclui um buffer para processos temporários. O tamanho do buffer necessário pode ser diferente no seu site.

Use a fórmula em Figura 17 para estimar o número máximo de processos usados pelo STCRSE, o RSED iniciou o ID do usuário da tarefa (não contando os processos temporários não documentados).

$$4 + 3 * A$$

Figura 17. Número de processos para STCRSE

Em que,

- "4" é igual ao número de processos usados pelo daemon RSE e espaços de endereço de RSE APF autorizado.
- "A" representa o número de espaços de endereço de conjunto de encadeamentos do RSE.

Use a fórmula em Figura 18 para estimar o número máximo de processos usados por um cliente Developer for System z (não contando os processos temporários não documentados).

$$(x + y + z) + 5 * s$$

Figura 18. Número de processos por cliente

Em que,

- "x" depende das opções de configuração selecionadas e é documentado na fórmula para calcular o número máximo de processos (Figura 16 na página 84).
- "y" depende das opções de configuração selecionadas e é documentado na fórmula para calcular o número máximo de processos (Figura 16 na página 84).
- "z" é 0 por padrão, mas pode aumentar dependendo das ações do usuário, conforme documentado na fórmula para calcular o número máximo de processos (Figura 16 na página 84).
- "s" é 1 quando o SCLM Developer Toolkit for usado ou, senão, 0.

As definições na Tabela 28 na página 86 podem limitar o número real de processos.

**Tabela 28. Limites do processo**

| Local         | Limite      | Recursos afetados                                  |
|---------------|-------------|----------------------------------------------------|
| BPXPRMxx      | MAXPROCSYS  | Limita o número total de processos                 |
| BPXPRMxx      | MAXPROCUSER | Limita o número de processos por UID do z/OS UNIX  |
| Segmento OMVS | PROCUSERMAX | Limita o número de processos para um ID do usuário |

Nota:

- O daemon RSE e os conjuntos de encadeamento do RSE usam o mesmo ID do usuário. Como o daemon RSE começa um novo conjunto de encadeamento sempre que for necessário, o número de processos para este ID do usuário pode aumentar. Portanto, MAXPROCUSER deve ser definido para acomodar esse crescimento, que pode ser formulado como  $3 + 2 \cdot A$ .
- O limite MAXPROCUSER é por ID de usuário (UID) exclusivo z/OS UNIX. Multiplique a contagem do processo por usuário estimada pelo número de clientes ativos simultaneamente se os seus usuários compartilharem o mesmo UID.
- O limite PROCUSERMAX é exclusivo por ID de usuário e é definido em seu software de segurança, no segmento OMVS do ID do usuário.

## Contagem de encadeamentos

Tabela 29 lista o número de encadeamentos usados pelas funções selecionadas do Developer for System z. "u" nas colunas "Encadeamentos" indica que a quantidade deve ser multiplicada pelo número de usuários ativos simultaneamente usando a função. A contagem de encadeamento é listada por processo, à medida que os limites são definidos neste nível.

- RSEDx: Esses encadeamentos são criados no conjunto de encadeamento do RSE, que é compartilhado por vários clientes. Todos os encadeamentos que terminam no mesmo conjunto de encadeamento devem ser incluídos juntos para obter a contagem total.
- Ativo: Esses encadeamentos fazem parte do processo que realmente executa a função solicitada. Cada processo é uma unidade independente, de modo que não há necessidade de somar as contagens de encadeamento, mesmo se elas estiverem designadas ao mesmo ID do usuário, a menos que observado de outra forma.
- Autoinicialização: Os processos de autoinicialização são necessários para iniciar o processo real. Cada um possui 1 encadeamento e pode haver várias autoinicializações consecutivas. Não há necessidade de somas as contagens de encadeamentos.

**Tabela 29. Contagem de encadeamentos**

| Encadeamentos  |            |                   | ID do usuário | Descrição                                                           |
|----------------|------------|-------------------|---------------|---------------------------------------------------------------------|
| RSEDx          | Ativado    | Autoinicialização |               |                                                                     |
| -              | (f) 3 + 1u | -                 | STCJMON       | JES Job Monitor                                                     |
| -              | 4          | -                 | STCDBM        | Debug Manager                                                       |
| -              | 14         | 2                 | STCRSE        | Daemon RSE                                                          |
| -              | 1          | -                 | STCRSE        | RSE daemon APF autorizado                                           |
| (a,g) 12 + 8u  | -          | (a) 1             | STCRSE        | Conjunto de encadeamentos do RSE com mineradores encadeamento único |
| (a,g) 12 + 19u | -          | (a) 1             | STCRSE        | Conjunto de encadeamentos do RSE, com mineradores multiencadeados   |
| -              | (a) 1      | -                 | STCRSE        | APF do conjunto de encadeamentos do RSE autorizado                  |

Tabela 29. Contagem de encadeamentos (continuação)

| Encadeamentos |            |        | ID do usuário     | Descrição                                                 |
|---------------|------------|--------|-------------------|-----------------------------------------------------------|
| -             | (b) 4u     | (b) 1u | <userid>          | ISPF Client Gateway (Serviço do TSO Commands e do SCLMDT) |
| -             | 2u         | -      | <userid>          | Serviço do TSO Commands (APPC)                            |
| 1u            | 2u         | -      | STCRSE e <userid> | CARMA (batch)                                             |
| 1u            | 2u         | -      | STCRSE e <userid> | CARMA (crastart)                                          |
| 2u            | (1+1+1+1)u | 1u     | STCRSE e <userid> | CARMA (crastart com rastreo) (h)                          |
| 5u            | 4u         | 3u     | STCRSE e <userid> | CARMA (ispf, descontinuado)                               |
| -             | (c) 1u     | 2u     | <userid>          | Build z/OS UNIX (comandos do shell)                       |
| 6u            | 1u         | -      | STCRSE e <userid> | Shell do z/OS UNIX                                        |
| (d) 1         | -          | -      | STCRSE            | Fazer Download                                            |
| (e) 1         | -          | -      | STCRSE            | Procurar                                                  |
| -             | (5)        | -      | <userid>          | SCLM Developer Toolkit                                    |
| 1u            | -          | -      | STCRSE            | Cronômetro para tempo limite inativo                      |

**Nota:**

- (a) Existe pelo menos 1 espaço de endereço do conjunto de encadeamento do RSE ativo. Consulte “Contagem do espaço de endereço” na página 81 para determinar o número real de espaços de endereços do conjunto de encadeamento do RSE.
- (b) Em situações normais e ao usar as opções de configuração padrão, existe 1 ISPF Client Gateway ativo por usuário. O número real pode variar, conforme descrito em “Contagem do espaço de endereço” na página 81.
- O SCLMDT exige um espaço de endereço do ISPF Client Gateway. O SCLMDT compartilha o espaço de endereço com o serviço do TSO Commands.
- Dependendo da ação selecionada, o SCLMDT pode usar vários processos de encadeamento único que terminam na conclusão da tarefa. A Tabela 29 na página 86 lista o número máximo de encadeamentos SCLMDT simultâneos.
- A maioria das ações relacionadas ao conjunto de dados do MVS usa o serviço do TSO Commands, que pode estar ativo no ISPF Client Gateway ou em uma transação do APPC, respectivamente.
- (c) Um build z/OS UNIX invoca utilitários de build diferentes, que podem ser multiencadeados. A Tabela 29 na página 86 lista o número mínimo de encadeamentos de build z/OS UNIX simultâneos.
- (d) Cada download de dados de host usará um encadeamento separado. Este encadeamento será encerrado quando os dados forem transferidos ao cliente.
- (e) Cada procura remota usará um encadeamento separado. Este encadeamento será encerrado quando os resultados forem transferidos ao cliente.
- Todos os encadeamentos listados permanecem ativos até que o processo relacionado termine, a menos que indicado de outra forma.
- A contagem normal de encadeamentos para o código autorizado pelo APF RSE é 1. Entretanto, durante a inicialização, há 13 ou mais encadeamentos ativos simultâneos temporariamente.
- (f) Um usuário único pode ter vários encadeamentos ativos no JES Job Monitor para permitir o processamento simultâneo de várias solicitações.
- (g) Mineiros específicos do usuário podem ser iniciados de duas maneiras; todos os mineradores de um único usuário podem compartilhar um único encadeamento (modo de encadeamento único dubbed), ou cada minerador usa um encadeamento dedicado (modo multiencadeado dubbed). Agrupar todos os

mineradores para um usuário em um encadeamento único reduz o uso do encadeamento dentro de um conjunto de encadeamentos, mas pode causar atrasos no processamento de comandos quando um usuário estiver executando multitarefas. O método de inicialização é controlado pela diretiva `DSTORE_USE_THREADED_MINERS` em `rzed.envvars`. A amostra `rzed.envvars` usa o modo multiencadeado.

- (h) rastreamento de inicialização do CARMA CRSTART é controlado pelo nível de depuração de RSE ativo para o `rsecomm.log`.

Use a fórmula na Figura 19 para estimar o número máximo de encadeamentos usados por um conjunto de encadeamentos RSE em uma configuração de minerador de único encadeamento. Use a fórmula em Figura 20 para estimar o número máximo de encadeamentos usados por um conjunto de encadeamentos do RSE em uma configuração de minerador multiencadeado. Use a fórmula da Figura 21 para avaliar o número máximo de encadeamentos usados pelo JES Job Monitor. Use a fórmula em Figura 22 para estimar o número máximo de encadeamentos usados pelo Debug Manager.

$$12 + N * (8 + x + y + z) + (20 + N * 0.1)$$

Figura 19. O número máximo de encadeamentos do conjunto de encadeamentos do RSE (mineradores de único encadeamento)

$$12 + N * (19 + x + y + z) + (20 + N * 0.1)$$

Figura 20. Número máximo de encadeamentos do conjunto de encadeamentos do RSE (mineradores multiencadeados)

$$3 + N + (20 + N * 0.1)$$

Figura 21. Número máximo de encadeamentos do JES Job Monitor

$$4$$

Figura 22. Número máximo de encadeamentos do Debug Manager

Em que,

- "N" representa o número máximo de usuários simultâneos neste conjunto de encadeamentos ou JES Job Monitor. As configurações padrão são planejadas para 30 usuários por conjunto de encadeamentos.
- "x" é um dos seguintes valores, dependendo das opções de configuração selecionadas.

| X | SCLMDT | TSO por meio do Client Gateway | TSO por meio do APFC | Tempo limite |
|---|--------|--------------------------------|----------------------|--------------|
| 0 | Não    | Não                            | Sim                  | Não          |
| 0 | Não    | Sim                            | Não                  | Não          |
| 0 | Sim    | Sim                            | Não                  | Não          |
| 1 | Não    | Não                            | Sim                  | Sim          |
| 1 | Não    | Sim                            | Não                  | Sim          |
| 1 | Sim    | Sim                            | Não                  | Sim          |

- “y” é um dos seguintes valores, dependendo das opções de configuração selecionadas.

| S |                               |
|---|-------------------------------|
| 0 | Sem CARMA                     |
| 1 | CARMA (batch)                 |
| 1 | CARMA (crastart)              |
| 2 | CARMA (crastart com rastreio) |
| 5 | CARMA (ispf, descontinuado)   |

- “z” é 0 por padrão, mas pode aumentar dependendo das ações do usuário:
  - Inclua 6 quando um shell z/OS UNIX for aberto. Esses encadeamentos permanecem ativos até que o usuário efetue logoff.
- “20 + N\*0.1” inclui um buffer para encadeamentos temporários. O tamanho do buffer necessário pode ser diferente no seu site. Diversos downloads e procuras simultâneos são dois exemplos que podem requerer que você aumente o tamanho deste buffer.

As definições na Tabela 30 podem limitar o número real de encadeamentos em um processo, o que é da maior importância para os conjuntos de encadeamentos do RSE.

*Tabela 30. Limites de encadeamento*

| Local         | Limite          | Recursos afetados                                                                                                                                               |
|---------------|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Segmento OMVS | THREADSMAX      | Limita o número de encadeamentos para um ID de usuário                                                                                                          |
| BPXPRMxx      | MAXTHREADS      | Limita o número de encadeamentos em um processo.                                                                                                                |
| BPXPRMxx      | MAXTHREADTASKS  | Limita o número de tarefas MVS em um processo.                                                                                                                  |
| BPXPRMxx      | MAXASSIZE       | Limita o tamanho de espaço de endereço e, portanto, o armazenamento disponível para blocos de controle relacionados a encadeamento.                             |
| rsed.envvars  | Xmx             | Define o tamanho máximo do heap Java. Este armazenamento é reservado e, portanto, não está mais disponível para blocos de controle relacionados a encadeamento. |
| rsed.envvars  | maximum.clients | Limita o número de clientes (e, portanto, seus encadeamentos) em um conjunto de encadeamento do RSE.                                                            |
| rsed.envvars  | maximum.threads | Limita o número de encadeamentos de cliente em um conjunto de encadeamentos RSE.                                                                                |
| FEJJCNFG      | MAX_THREADS     | Limita o número de encadeamentos no JES Job Monitor.                                                                                                            |

#### Nota:

- O limite THREADSMAX é exclusivo por ID do usuário e é definido em seu software de segurança, no segmento OMVS do ID do usuário.
- O valor para maximum.threads em rsed.envvars deve ser mais baixo do que o valor para MAXTHREADS e MAXTHREADTASKS em BPXPRMxx, e THREADSMAX no segmento OMVS do ID do usuário da tarefa iniciada do RSED.
- O comando operador **DISPLAY PROCESS,CPU**, que mostra os encadeamentos ativos em um conjunto de encadeamentos, está limitado a mostrar apenas os primeiros 4.000 encadeamentos.

## Uso temporário de recursos

O uso de recurso documentado nas seções anteriores é permanente para o tempo de vida do Developer for System z ou semipermanente para certas tarefas específicas do usuário.

Entretanto, o Developer for System z usará temporariamente os recursos adicionais para tarefas de manutenção e atender às solicitações a seguir:



- O processamento de um evento de arquivo de auditoria (diretiva `audit.action` em `rzed.envvars`) usa um encadeamento adicional, um processo adicional e possivelmente (se `audit.action.id` estiver configurado) um espaço de endereço adicional.
- O processamento de um evento de logon (diretiva `logon.action` em `rzed.envvars`) usa um encadeamento adicional, um processo adicional e possivelmente (se `logon.action.id` estiver configurado) um espaço de endereço adicional.
- O comando do operador IVP PASSTICKET usará dois encadeamentos adicionais.
- O comando do operador IVP DAEMON usará um encadeamento adicional, um processo adicional e um espaço de endereço adicional.
- O comando do operador IVP ISPF usará um encadeamento adicional, um processo adicional e um espaço de endereço adicional, além dos recursos usados pelo Gateway do Cliente ISPF.

## Contagem de encadeamentos

Tabela 29 na página 86 lista o número de encadeamentos usados pelas funções selecionadas do Developer for System z. "u" nas colunas "Encadeamentos" indica que a quantidade deve ser multiplicada pelo número de usuários ativos simultaneamente usando a função. A contagem de encadeamento é listada por processo, à medida que os limites são definidos neste nível.

- RSEDx: Esses encadeamentos são criados no conjunto de encadeamento do RSE, que é compartilhado por vários clientes. Todos os encadeamentos que terminam no mesmo conjunto de encadeamento devem ser incluídos juntos para obter a contagem total.
- Ativo: Esses encadeamentos fazem parte do processo que realmente executa a função solicitada. Cada processo é uma unidade independente, de modo que não há necessidade de somar as contagens de encadeamento, mesmo se elas estiverem designadas ao mesmo ID do usuário, a menos que observado de outra forma.
- Autoinicialização: Os processos de autoinicialização são necessários para iniciar o processo real. Cada um possui 1 encadeamento e pode haver várias autoinicializações consecutivas. Não há necessidade de somas as contagens de encadeamentos.

*Tabela 31. Contagem de encadeamentos*

| Encadeamentos  |            |                   | ID do usuário     | Descrição                                                           |
|----------------|------------|-------------------|-------------------|---------------------------------------------------------------------|
| RSEDx          | Ativado    | Autoinicialização |                   |                                                                     |
| -              | (f) 3 + 1u | -                 | STCJMON           | JES Job Monitor                                                     |
| -              | 4          | -                 | STCDBM            | Debug Manager                                                       |
| -              | 14         | 2                 | STCRSE            | Daemon RSE                                                          |
| -              | 1          | -                 | STCRSE            | RSE daemon APF autorizado                                           |
| (a,g) 12 + 8u  | -          | (a) 1             | STCRSE            | Conjunto de encadeamentos do RSE com mineradores encadeamento único |
| (a,g) 12 + 19u | -          | (a) 1             | STCRSE            | Conjunto de encadeamentos do RSE, com mineradores multiencadeados   |
| -              | (a) 1      | -                 | STCRSE            | APF do conjunto de encadeamentos do RSE autorizado                  |
| -              | (b) 4u     | (b) 1u            | <userid>          | ISPF Client Gateway (Serviço do TSO Commands e do SCLMDT)           |
| -              | 2u         | -                 | <userid>          | Serviço do TSO Commands (APPC)                                      |
| 1u             | 2u         | -                 | STCRSE e <userid> | CARMA (batch)                                                       |

Tabela 31. Contagem de encadeamentos (continuação)

| Encadeamentos |            |    | ID do usuário     | Descrição                            |
|---------------|------------|----|-------------------|--------------------------------------|
| 1u            | 2u         | -  | STCRSE e <userid> | CARMA (crastart)                     |
| 2u            | (1+1+1+1)u | 1u | STCRSE e <userid> | CARMA (crastart com rastreio) (h)    |
| 5u            | 4u         | 3u | STCRSE e <userid> | CARMA (ispf, descontinuado)          |
| -             | (c) 1u     | 2u | <userid>          | Build z/OS UNIX (comandos do shell)  |
| 6u            | 1u         | -  | STCRSE e <userid> | Shell do z/OS UNIX                   |
| (d) 1         | -          | -  | STCRSE            | Fazer Download                       |
| (e) 1         | -          | -  | STCRSE            | Procurar                             |
| -             | (5)        | -  | <userid>          | SCLM Developer Toolkit               |
| 1u            | -          | -  | STCRSE            | Cronômetro para tempo limite inativo |

**Nota:**

- (a) Existe pelo menos 1 espaço de endereço do conjunto de encadeamento do RSE ativo. Consulte “Contagem do espaço de endereço” na página 81 para determinar o número real de espaços de endereços do conjunto de encadeamento do RSE.
- (b) Em situações normais e ao usar as opções de configuração padrão, existe 1 ISPF Client Gateway ativo por usuário. O número real pode variar, conforme descrito em “Contagem do espaço de endereço” na página 81.
- O SCLMDT exige um espaço de endereço do ISPF Client Gateway. O SCLMDT compartilha o espaço de endereço com o serviço do TSO Commands.
- Dependendo da ação selecionada, o SCLMDT pode usar vários processos de encadeamento único que terminam na conclusão da tarefa. A Tabela 29 na página 86 lista o número máximo de encadeamentos SCLMDT simultâneos.
- A maioria das ações relacionadas ao conjunto de dados do MVS usa o serviço do TSO Commands, que pode estar ativo no ISPF Client Gateway ou em uma transação do APPC, respectivamente.
- (c) Um build z/OS UNIX invoca utilitários de build diferentes, que podem ser multiencadeados. A Tabela 29 na página 86 lista o número mínimo de encadeamentos de build z/OS UNIX simultâneos.
- (d) Cada download de dados de host usará um encadeamento separado. Este encadeamento será encerrado quando os dados forem transferidos ao cliente.
- (e) Cada procura remota usará um encadeamento separado. Este encadeamento será encerrado quando os resultados forem transferidos ao cliente.
- Todos os encadeamentos listados permanecem ativos até que o processo relacionado termine, a menos que indicado de outra forma.
- A contagem normal de encadeamentos para o código autorizado pelo APF RSE é 1. Entretanto, durante a inicialização, há 13 ou mais encadeamentos ativos simultâneos temporariamente.
- (f) Um usuário único pode ter vários encadeamentos ativos no JES Job Monitor para permitir o processamento simultâneo de várias solicitações.
- (g) Mineiros específicos do usuário podem ser iniciados de duas maneiras; todos os mineradores de um único usuário podem compartilhar um único encadeamento (modo de encadeamento único dubbed), ou cada minerador usa um encadeamento dedicado (modo multiencadeado dubbed). Agrupar todos os mineradores para um usuário em um encadeamento único reduz o uso do encadeamento dentro de um conjunto de encadeamentos, mas pode causar atrasos no processamento de comandos quando um usuário estiver executando

multitarefa. O método de inicialização é controlado pela diretiva `DSTORE_USE_THREADED_MINERS` em `rsed.envvars`. A amostra `rsed.envvars` usa o modo multiencadeado.

- (h) rastreamento de inicialização do CARMA CRSTART é controlado pelo nível de depuração de RSE ativo para o `rsecomm.log`.

Use a fórmula na Figura 19 na página 88 para estimar o número máximo de encadeamentos usados por um conjunto de encadeamentos RSE em uma configuração de minerador de único encadeamento. Use a fórmula em Figura 20 na página 88 para estimar o número máximo de encadeamentos usados por um conjunto de encadeamentos do RSE em uma configuração de minerador multiencadeado. Use a fórmula da Figura 21 na página 88 para avaliar o número máximo de encadeamentos usados pelo JES Job Monitor. Use a fórmula em Figura 22 na página 88 para estimar o número máximo de encadeamentos usados pelo Debug Manager.

$$12 + N * (8 + x + y + z) + (20 + N * 0.1)$$

Figura 23. O número máximo de encadeamentos do conjunto de encadeamentos do RSE (mineradores de único encadeamento)

$$12 + N * (19 + x + y + z) + (20 + N * 0.1)$$

Figura 24. Número máximo de encadeamentos do conjunto de encadeamentos do RSE (mineradores multiencadeados)

$$3 + N + (20 + N * 0.1)$$

Figura 25. Número máximo de encadeamentos do JES Job Monitor

$$4$$

Figura 26. Número máximo de encadeamentos do Debug Manager

Em que,

- "N" representa o número máximo de usuários simultâneos neste conjunto de encadeamentos ou JES Job Monitor. As configurações padrão são planejadas para 30 usuários por conjunto de encadeamentos.
- "x" é um dos seguintes valores, dependendo das opções de configuração selecionadas.

| X | SCLMDT | TSO por meio do Client Gateway | TSO por meio do APFC | Tempo limite |
|---|--------|--------------------------------|----------------------|--------------|
| 0 | Não    | Não                            | Sim                  | Não          |
| 0 | Não    | Sim                            | Não                  | Não          |
| 0 | Sim    | Sim                            | Não                  | Não          |
| 1 | Não    | Não                            | Sim                  | Sim          |
| 1 | Não    | Sim                            | Não                  | Sim          |
| 1 | Sim    | Sim                            | Não                  | Sim          |

- "y" é um dos seguintes valores, dependendo das opções de configuração selecionadas.

|   |                               |
|---|-------------------------------|
| S |                               |
| 0 | Sem CARMA                     |
| 1 | CARMA (batch)                 |
| 1 | CARMA (crastart)              |
| 2 | CARMA (crastart com rastreio) |
| 5 | CARMA (ispf, descontinuado)   |

- “z” é 0 por padrão, mas pode aumentar dependendo das ações do usuário:
  - Inclua 6 quando um shell z/OS UNIX for aberto. Esses encadeamentos permanecem ativos até que o usuário efetue logoff.
- “20 + N\*0.1” inclui um buffer para encadeamentos temporários. O tamanho do buffer necessário pode ser diferente no seu site. Diversos downloads e procuras simultâneos são dois exemplos que podem requerer que você aumente o tamanho deste buffer.

As definições na Tabela 30 na página 89 podem limitar o número real de encadeamentos em um processo, o que é da maior importância para os conjuntos de encadeamentos do RSE.

*Tabela 32. Limites de encadeamento*

| Local         | Limite          | Recursos afetados                                                                                                                                               |
|---------------|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Segmento OMVS | THREADSMAX      | Limita o número de encadeamentos para um ID de usuário                                                                                                          |
| BPXPRMxx      | MAXTHREADS      | Limita o número de encadeamentos em um processo.                                                                                                                |
| BPXPRMxx      | MAXTHREADTASKS  | Limita o número de tarefas MVS em um processo.                                                                                                                  |
| BPXPRMxx      | MAXASSIZE       | Limita o tamanho de espaço de endereço e, portanto, o armazenamento disponível para blocos de controle relacionados a encadeamento.                             |
| rsed.envvars  | Xmx             | Define o tamanho máximo do heap Java. Este armazenamento é reservado e, portanto, não está mais disponível para blocos de controle relacionados a encadeamento. |
| rsed.envvars  | maximum.clients | Limita o número de clientes (e, portanto, seus encadeamentos) em um conjunto de encadeamento do RSE.                                                            |
| rsed.envvars  | maximum.threads | Limita o número de encadeamentos de cliente em um conjunto de encadeamentos RSE.                                                                                |
| FEJCNFG       | MAX_THREADS     | Limita o número de encadeamentos no JES Job Monitor.                                                                                                            |

**Nota:**

- O limite THREADSMAX é exclusivo por ID do usuário e é definido em seu software de segurança, no segmento OMVS do ID do usuário.
- O valor para maximum.threads em rsed.envvars deve ser mais baixo do que o valor para MAXTHREADS e MAXTHREADTASKS em BPXPRMxx, e THREADSMAX no segmento OMVS do ID do usuário da tarefa iniciada do RSED.
- O comando operador **DISPLAY PROCESS,CPU**, que mostra os encadeamentos ativos em um conjunto de encadeamentos, está limitado a mostrar apenas os primeiros 4.000 encadeamentos.

## Uso de Armazenamento

RSE é um aplicativo Java, que implica que o planejamento de uso de armazenamento (memória) para Developer for System z deve levar dois limites de alocação de armazenamento em consideração, tamanho de heap Java e tamanho de Espaço de Endereço.

### Limite de Tamanho de Heap Java

Java oferece vários serviços para facilitar os esforços de codificação para aplicativos Java. Um desses serviços é o gerenciamento de armazenamento.

O gerenciamento de armazenamento Java aloca grandes blocos de armazenamento e os usa para pedidos de armazenamento pelo aplicativo. Esse armazenamento gerenciado por Java é chamado de heap Java. A coleta de lixo periódica (desfragmentação) reclama o espaço não utilizado no heap e reduz o seu tamanho. Note que, para salvar ciclos de CPU, a coleta de lixo tende a aguardar até que o armazenamento ocupado seja realmente necessário, deixando, assim, o armazenamento que não é mais usado alocado (e se tornando paginado) por um período maior de tempo do que o absolutamente necessário.

O tamanho de heap máximo Java é definido em `rse.envvars` com a diretiva `Xmx`. Se esta diretiva não for especificada, o Java usará um tamanho padrão de 512 MB. Você deve especificar um valor de 256 MB ou mais alto. Ao executar em modo de 64 bits, o Java tentará alocar o heap acima de 2 GB de barramento, liberando espaço abaixo do barramento.

Cada conjunto de armazenamento do RSE (que atende às ações do cliente) é um aplicativo Java separado e, portanto, tem um heap Java pessoal. Observe que todos os conjuntos de encadeamento usam o mesmo arquivo de configuração `rse.envvars` e, portanto, têm o mesmo limite de tamanho de heap Java.

O uso do conjunto de encadeamento do heap Java depende muito das ações executadas pelos clientes conectados. O monitoramento regular do uso de heap é necessário para definir o limite de tamanho de heap ideal. Use o comando do operador **modificar processo de exibição** para monitorar o uso de heap Java por conjuntos de encadeamento do RSE.

## Limite de Tamanho do Espaço de Endereço

Todos os aplicativos z/OS, incluindo aplicativos Java, estão ativos dentro de um espaço de endereço, e estão, portanto, ligados pelas limitações de tamanho do espaço de endereço.

O tamanho do espaço de endereço desejado é especificado durante a inicialização, por exemplo, com o parâmetro `REGION` em JCL. Entretanto, as configurações do sistema podem limitar o tamanho do espaço de endereço real. Consulte “Tamanho do espaço de endereço” na página 179 para saber mais sobre esses limites.

- `MAXASSIZE` em `SYS1.PARMLIB(BPXPRMxx)`
- `ASSIZEMAX` no segmento OMVS do ID do usuário designado à tarefa iniciada
- saídas do sistema IEFUSI e IEALIMIT
- `MEMLIMIT` in `SYS1.PARMLIB(SMFPRMxx)` para modo de endereçamento de 64 bits

Os conjuntos de encadeamento do RSE herdam os limites de tamanho do espaço de endereço do daemon RSE. O tamanho do espaço de endereço deve ser suficiente para abrigar o heap Java, o próprio Java, as áreas de armazenamento comuns e todos os blocos de controle que o sistema cria para suportar a atividade do conjunto de encadeamento, como um TCB (Bloco de Controle de Tarefa) por encadeamento. Observe que algum desse uso de armazenamento está abaixo da linha de 16 MB. Ao executar em modo de 64 bits, o Java tentará alocar o heap acima de 2 GB de barramento, liberando espaço abaixo do barramento.

Você deve monitorar o tamanho do espaço de endereço real antes de alterar quaisquer configurações que o influenciem, como alterar o tamanho do heap Java ou a quantidade de usuários suportada por um único conjunto de encadeamento. Use o software de monitoramento regular do sistema para controlar o uso de armazenamento real pelo Developer for system z. Se você não tiver uma

ferramenta de monitoramento dedicada, então informações básicas podem ser reunidas com ferramentas como a visualização SDSF DA ou TASID (uma ferramenta de informações do sistema como elas estão armazenadas no banco de dados disponível por meio da página da Web "Support and downloads" do ISPF).

## Diretrizes de Estimativa de Tamanho

Conforme mencionado antes, o uso de armazenamento real pelo Developer para System z é altamente influenciado pela atividade do usuário. Algumas ações usam uma quantidade fixa de armazenamento (por exemplo, logon), enquanto outras são variáveis (por exemplo, listando conjuntos de dados com um qualificador de alto nível especificado).

- Use um espaço de endereço de 2 GB para RSE para permitir espaço para o heap Java e todos os blocos de controle do sistema.
- Ao executar em modo de 64 bits, certifique-se de que o armazenamento acima de 2 GB de barramento esteja realmente disponível para RSE.
- Consulte "Tamanho do espaço de endereço" na página 179 para saber mais sobre onde os limites de tamanho de espaço de endereço podem ser configurados.
- A configuração `rsed.envvars` de amostra é planejada para 30 usuários por conjunto de encadeamentos.
  - `maximum.clients=30`
  - `maximum.threads=520` ( $10+17*30 = 520$ , portanto 520 permitem 30 clientes)
- A configuração `rsed.envvars` de amostra permite que o heap Java cresça até 512 MB. Isso permite 30 clientes usando uma média de 17 MB por cliente ( $30*17 = 510$ ).

Observe que o RSE exibe o heap Java atual e o limite de tamanho de espaço de endereço durante a inicialização na mensagem do console FEK004I.

Use um dos seguintes cenários se o monitoramento mostrar que o tamanho de heap Java atual é insuficiente para a carga de trabalho real:

- Aumente o tamanho de heap Java máximo com a diretiva `Xmx` em `rsed.envvars`. Antes de fazer isso, verifique se há espaço no espaço de endereço para o aumento de tamanho.
- Diminua o número máximo de clientes por conjunto de encadeamentos com a diretiva `maximum.clients` em `rsed.envvars`. O RSE ainda suportará o mesmo número de clientes, mas os clientes serão distribuídos entre mais conjuntos de encadeamento.

Como referência, a Tabela 33 mostra valores usados por clientes reais do Developer for System z para configurações de chave `rsed.envvars` que têm impacto no uso de armazenamento.

*Tabela 33. Configurações de Referência para Uso de Armazenamento*

| mxm (heap java máximo) | maximum.clients | Tipo de desenvolvimento primário |
|------------------------|-----------------|----------------------------------|
| 512M                   | 30              | PL/I                             |
| 512M                   | 10              | COBOL                            |
| 384M                   | 12              | COBOL                            |
| 800M (64 bits)         | 20              | Não especificado                 |

## Análise do Uso de Armazenamento de Amostra

As exibições nas figuras a seguir mostram alguns números de uso de recurso de amostra para uma configuração padrão do Developer for System z com essas modificações.

- single.logon está desativado para impedir que o RSE crie, pelo menos, 2 espaços de endereço de conjunto de encadeamentos
- O tamanho máximo de heap Java é definido como 10 MB, uma vez que um máximo pequeno resultará em um uso percentil maior e os limites do tamanho de heap serão atingidos com mais rapidez.

Tamanho Máx Heap=10 MB e privado AS Tamanho=1,959 MB

Inicialização

BPXM023I (STCRSE)  
ID do Processo(268 ) Uso de Memória(7%) Clientes(0)

| Nome Tarefa | Tempo de CPU | Armazen. | EXCP  |
|-------------|--------------|----------|-------|
| JMON        | 0,01         | 2740     | 72    |
| RSED        | 4,47         | 32,8 M   | 15910 |
| RSED8       | 1,15         | 27,4 M   | 12612 |

logon 1

BPXM023I (STCRSE)  
ID do Processo(268 ) Uso de Memória(13%) Clientes(1)

| Nome Tarefa | Tempo de CPU | Armazen. | EXCP  |
|-------------|--------------|----------|-------|
| JMON        | 0,01         | 2864     | 81    |
| RSED        | 4,55         | 32,8 M   | 15980 |
| RSED8       | 3,72         | 55,9 M   | 24128 |

logon 2

BPXM023I (STCRSE)  
ID do Processo(268 ) Uso de Memória(23%) Clientes(2)

| Nome Tarefa | Tempo de CPU | Armazen. | EXCP  |
|-------------|--------------|----------|-------|
| JMON        | 0,02         | 2944     | 86    |
| RSED        | 4,58         | 32,9 M   | 16027 |
| RSED8       | 4,20         | 57,8 M   | 25205 |

logon 3

BPXM023I (STCRSE)  
ID do Processo(268 ) Uso de Memória(37%) Clientes(3)

| Nome Tarefa | Tempo de CPU | Armazen. | EXCP  |
|-------------|--------------|----------|-------|
| JMON        | 0,02         | 3020     | 91    |
| RSED        | 4,60         | 32,9 M   | 16076 |
| RSED8       | 4,51         | 59,6 M   | 26327 |

logon 4

BPXM023I (STCRSE)  
ID do Processo(268 ) Uso de Memória(41%) Clientes(4)

| Nome Tarefa | Tempo de CPU | Armazen. | EXCP  |
|-------------|--------------|----------|-------|
| JMON        | 0,02         | 3108     | 96    |
| RSED        | 4,61         | 32,9 M   | 16125 |
| RSED8       | 4,77         | 62,3 M   | 27404 |

Figura 27. Uso de recursos com 5 logons

logon 5

BPXM023I (STCRSE)  
ID do Processo(268 ) Uso de Memória(41%) Clientes(4)  
ID do Processo(33554706) Uso de Memória(13%) Clientes(1)

| Nome Tarefa | Tempo de CPU | Armazen. | EXCP  |
|-------------|--------------|----------|-------|
| JMON        | 0,03         | 3184     | 101   |
| RSED        | 4,64         | 32,9 M   | 16229 |
| RSED8       | 4,78         | 62,4 M   | 27413 |
| RSED9       | 4,60         | 56,6 M   | 24065 |

Figura 28. Uso de recursos com 5 logons (continuação)

A Figura 27 e a Figura 28 mostram um cenário em que 5 clientes efetuam logon em um daemon RSE com um heap Java de 10 MB.



- Um conjunto de encadeamento (RSED8) está em um estado inativo na inicialização, usando cerca de 27 MB, dos quais 0,7 MB estão no heap Java (7% de 10 MB).
- O conjunto de encadeamento se torna ativo quando o primeiro cliente se conecta, usando outros 27 MB mais 2 MB para cada cliente que se conecta.
- Parte desses 2 MB por conexão estarão no heap Java, como mostra o aumento no uso do heap.
- Entretanto, não há um padrão real no uso do heap, pois ele depende dos mecanismos Java que avaliam o armazenamento necessário e alocam mais do que o necessário. A coleta de lixo intermitente libera o armazenamento, tornando as tendências ainda mais difíceis de serem detectadas.
- Mecanismos internos que limitam o número de conexões por conjunto de encadeamento para garantir tamanho de heap suficiente para os encadeamentos ativos resultam na quinta conexão que está sendo criada em um novo conjunto de encadeamento (RSED9). Essas redes de segurança interna não são normalmente invocadas ao usar uma configuração configurada corretamente, pois outros limites serão atingidos primeiro (a maioria provavelmente `maximum.clients` em `rsed.envvars`).

Tamanho Máx Heap=10 MB e privado AS Tamanho=1,959 MB

inicialização

BPXM023I (STCRSE)  
ID do Processo(212 ) Uso de Memória(7%) Clientes(0)

| Nome  | Tarefa | Tempo de CPU | Armazen. | EXCP  |
|-------|--------|--------------|----------|-------|
| JMON  |        | 0,01         | 2736     | 71    |
| RSED  |        | 4,35         | 32,9 M   | 15117 |
| RSED8 |        | 1,43         | 27,4 M   | 12609 |

logon

BPXM023I (STCRSE)  
ID do Processo(212 ) Uso de Memória(13%) Clientes(1)

| Nome  | Tarefa | Tempo de CPU | Armazen. | EXCP  |
|-------|--------|--------------|----------|-------|
| JMON  |        | 0,01         | 2864     | 80    |
| RSED  |        | 4,48         | 33,0 M   | 15187 |
| RSED8 |        | 3,53         | 53,9 M   | 24125 |

expandir árvore MVS grande (195 conjuntos de dados)

BPXM023I (STCRSE)  
ID do Processo(212 ) Uso de Memória(13%) Clientes(1)

| Nome  | Tarefa | Tempo de CPU | Armazen. | EXCP  |
|-------|--------|--------------|----------|-------|
| JMON  |        | 0,01         | 2864     | 80    |
| RSED  |        | 4,58         | 33,1 M   | 16094 |
| RSED8 |        | 4,28         | 56,1 M   | 24740 |

expandir PDS pequeno (21 membros)

BPXM023I (STCRSE)  
ID do Processo(212 ) Uso de Memória(13%) Clientes(1)

| Nome      | Tarefa | Tempo de CPU | Armazen. | EXCP  |
|-----------|--------|--------------|----------|-------|
| IBMUUSER2 |        | 0,22         | 2644     | 870   |
| JMON      |        | 0,01         | 2864     | 80    |
| RSED      |        | 4,61         | 33,1 M   | 16108 |
| RSED8     |        | 4,40         | 56,2 M   | 24937 |

abrir membro de tamanho médio (86 linhas)

BPXM023I (STCRSE)  
ID do Processo(212 ) Uso de Memória(13%) Clientes(1)

| Nome      | Tarefa | Tempo de CPU | Armazen. | EXCP  |
|-----------|--------|--------------|----------|-------|
| IBMUUSER2 |        | 0,22         | 2644     | 870   |
| JMON      |        | 0,01         | 2864     | 80    |
| RSED      |        | 4,61         | 33,1 M   | 16108 |
| RSED8     |        | 8,12         | 62,7 M   | 27044 |

Figura 29. Uso de recursos ao editar um membro PDS

A Figura 29 mostra um cenário em que 1 cliente efetua logon em um daemon RSE com um heap Java de 10 MB e edita um membro PDS.



- A procura no catálogo que resulta em 195 nomes de conjuntos de dados usou cerca de 2MB de armazenamento, tudo devido à atividade do sistema, pois o uso do heap Java não aumenta.
- A abertura do PDS de 21 membros dificilmente usa alguma memória do conjunto de encadeamento, mas a tela mostra que o serviço TSO Commands foi invocado. Há um novo espaço de endereço ativo (IBMUSER2), que usa o tamanho da região designado a esse ID do usuário em TSO. Esse espaço de endereço permanece ativo por uma quantidade de tempo específica, de modo que ele pode ser reutilizado em pedidos futuros pelo serviço TSO Commands.
- A abertura de um membro mostra números semelhantes enquanto expande um qualificador de alto nível. O uso do heap Java permanece o mesmo, mas há um aumento no armazenamento de 6,5 MB devido à atividade do sistema.

---

## Uso do espaço do sistema de arquivos z/OS UNIX

A maioria dos dados relacionados ao Developer for System z que não estão gravados em uma instrução DD terminam em um arquivo z/OS UNIX. O programador de sistema tem controle sobre os dados que são gravados e para onde eles vão. Entretanto, não há controle sobre a quantidade de dados gravada.

Os dados podem ser agrupados nas seguintes categorias:

- Análise do problema (arquivos de log e de dump do sistema), no qual vários detalhes são documentados no Capítulo 12, “Resolução de problemas de configuração”, na página 163
- Auditoria, conforme documentado em “Criação de Log de Auditoria” na página 24
- Metadados push-to-client, conforme documentado em “Metadados Push-to-client” na página 120.
- Dados temporários

Conforme documentado em Capítulo 12, “Resolução de problemas de configuração”, na página 163, o Developer for System z grava os logs de host relacionados a RSE nos seguintes diretórios z/OS UNIX:

- /var/rdz/logs/server para os logs da tarefa iniciada do RSE
- /var/rdz/logs/\$LOGNAME para logs do usuário

Por padrão, apenas as mensagens de erro e de aviso são gravadas nos logs. Portanto, se tudo correr conforme o planejado, esses diretórios devem manter apenas os arquivos vazios ou quase vazios(sem contar os logs de auditoria).

Você pode ativar a criação de log de mensagens informativas, preferivelmente na direção do centro de suporte IBM, o que aumenta perceptivelmente o tamanho dos arquivos de log.

```

inicialização
$ ls -l /var/rdz/logs/server
total 144
-rw-rw-rw- 1 STCRSE STCGRP 33642 Jul 10 12:10 rsedaemon.log
-rw-rw-rw- 1 STCRSE STCGRP 1442 Jul 10 12:10 rseserver.log

logon
$ ls -l /var/rdz/logs/server
total 144
-rw----- 1 STCRSE STCGRP 36655 Jul 10 12:11 rsedaemon.log
-rw----- 1 STCRSE STCGRP 1893 Jul 10 12:11 rseserver.log
$ ls -l /var/rdz/logs/IBMUSER
total 160
-rw----- 1 IBMUSER SYS1 3459 Jul 10 12:11 ffs.log
-rw----- 1 IBMUSER SYS1 0 Jul 10 12:11 ffsget.log
-rw----- 1 IBMUSER SYS1 0 Jul 10 12:11 ffsput.log
-rw----- 1 IBMUSER SYS1 303 Jul 10 12:11 ffslock.log
-rw----- 1 IBMUSER SYS1 7266 Jul 10 12:11 rsecomm.log

logoff
$ ls -l /var/rdz/logs/server
total 80
-rw----- 1 STCRSE STCGRP 36655 Jul 10 12:11 rsedaemon.log
-rw----- 1 STCRSE STCGRP 2208 Jul 10 12:11 rseserver.log
$ ls -l /var/rdz/logs/IBMUSER
total 296
-rw----- 1 IBMUSER SYS1 6393 Jul 10 12:11 ffs.log
-rw----- 1 IBMUSER SYS1 0 Jul 10 12:11 ffsget.log
-rw----- 1 IBMUSER SYS1 0 Jul 10 12:11 ffsput.log
-rw----- 1 IBMUSER SYS1 609 Jul 10 12:11 ffslock.log
-rw----- 1 IBMUSER SYS1 45157 Jul 10 12:11 rsecomm.log

parar
$ ls -l /var/rdz/logs/server
total 80
-rw----- 1 STCRSE STCGRP 36655 Jul 10 12:11 rsedaemon.log
-rw----- 1 STCRSE STCGRP 2490 Jul 10 12:12 rseserver.log

```

Figura 30. Uso do espaço do sistema de arquivos z/OS UNIX

A Figura 30 mostra o uso mínimo do espaço do sistema de arquivos z/OS UNIX ao usar o nível de depuração 2 (mensagens informativas).

- Os logs de tarefas iniciadas usam 34 KB após a inicialização e crescem lentamente quando os usuários efetuam logon, efetuam logoff ou os comandos do operador são emitidos.
- Um diretório de log do cliente usa 11 KB após o logon e cresce em um ritmo uniforme quando o usuário começa a trabalhar (não mostrado no exemplo).
- Efetuar logoff incluir outros 40 KB nos logs do usuário, deixando-os com 51 KB.

Exceto para logs de auditoria, os arquivos de log são sobrescritos em cada reinício (para a tarefa iniciada do RSE) ou logon (de um cliente), mantendo o tamanho total em verificação. Os logs de auditoria são removidos após o intervalo especificado em `audit.retention.period` expirar. A diretiva `keep.last.log` em `rsed.envvars` altera isso ligeiramente, uma vez que ela pode instruir o RSE a manter uma cópia dos logs anteriores. As cópias mais antigas são sempre removidas. Se a diretiva `keep.all.logs` em `rsed.envvars` estiver ativada, todos os logs têm um registro de data e hora anexados ao seus nomes e os arquivos são removidos após o intervalo especificado em `log.retention.period` expirar.

Uma mensagem de aviso é enviada para o console quando o sistema de arquivos que contém os arquivos de log estiver em execução com pouco espaço livre. Essa mensagem do console (FEK103E) é repetida regularmente até que o problema de pouco espaço seja resolvido. Quando o sistema de arquivos ficar sem espaço, o RSE tentará excluir arquivos de log existentes para liberar espaço. Os logs de auditoria não são tocados por este processo.

As definições na Tabela 34 controlam os dados que são gravados nos diretórios de log e onde os diretórios estão localizados.

Tabela 34. Diretivas de saída do log

| Local                            | Diretriz                 | Funções                                    |
|----------------------------------|--------------------------|--------------------------------------------|
| <code>resecomm.properties</code> | <code>debug_level</code> | Definir o nível de detalhes do log padrão. |

**Tabela 34. Diretivas de saída do log (continuação)**

| Local               | Diretriz                                 | Funções                                                                                           |
|---------------------|------------------------------------------|---------------------------------------------------------------------------------------------------|
| rsecomm.properties  | USER                                     | Ativar o debug_level 2 para usuários especificados.                                               |
| rsed.envvars        | keep.all.logs                            | Manter uma cópia dos logs anteriores antes da inicialização/logon.                                |
| rsed.envvars        | keep.last.log                            | Manter uma cópia dos logs anteriores antes da inicialização/logon.                                |
| rsed.envvars        | enable.audit.log                         | Manter um rastreo de auditoria de ações do cliente.                                               |
| rsed.envvars        | enable.standard.log                      | Gravar os fluxos stdout e stderr do conjunto (ou conjuntos) de encadeamento em um arquivo de log. |
| rsed.envvars        | DSTORE_TRACING_ON                        | Ativar a criação de log de ações do DataStore.                                                    |
| rsed.envvars        | DSTORE_MEMLOGGING_ON                     | Ativar a criação de log do uso de memória do DataStore.                                           |
| Comando do operador | modify rsecommlog <level>                | Altera dinamicamente o nível de detalhes do log de rsecomm.log                                    |
| Comando do operador | modify rsedaemonlog <level>              | Altera dinamicamente o nível de detalhes do log de rsedaemon.log                                  |
| Comando do operador | modify rseserverlog <level>              | Altera dinamicamente o nível de detalhe do log de rseserver.log                                   |
| Comando do operador | modificar rsestandardlog {on   off}      | Altera dinamicamente a atualização de std*.log                                                    |
| Comando do operador | modificar rastreo {on   off} USER=userid | Ativar o debug_level 2 para usuários especificados.                                               |
| Comando do operador | modificar rastreo {on   off} SERVER=pid  | Ativar o debug_level 2 para usuários especificados.                                               |
| Comando do operador | modificar a limpeza de rastreo           | Desativar a instalação de rastreo.                                                                |
| Comando do operador | modificar logs                           | Coletar logs de host e informações de configuração                                                |
| rsed.envvars        | daemon.log                               | Caminho inicial para a tarefa iniciada do RSE e os logs de auditoria.                             |
| rsed.envvars        | user.log                                 | Caminho inicial para logs do usuário.                                                             |
| rsed.envvars        | CGL_ISPWORK                              | Caminho inicial dos logs do ISPF Client Gateway                                                   |
| rsed.envvars        | TMPDIR                                   | Diretório para logs IVP e comando do operador <b>modify logs</b>                                  |
| rsed.envvars        | _CEE_DMPTARG                             | Diretório de dumps Java                                                                           |

Developer for System z, junto com o software de requisito, como o ISPF Client Gateway, também grava dados temporários no /tmp e /var/rdz/WORKAREA. A quantidade de dados gravada aqui como resultado de ações do usuário é imprevisível, portanto você deve ter um amplo espaço livre nos sistemas de arquivos que mantêm esses diretórios.

O Developer for System z sempre tenta limpar estes arquivos temporários, mas a limpeza manual, conforme documentado em "(Opcional) Limpeza de WORKAREA e /tmp" em *Guia de Configuração do Host* (SC23-7658), pode ser executada virtualmente a qualquer momento.

As definições na Tabela 35 controlam onde os diretórios de dados temporários estão localizados.

**Tabela 35. Diretivas de saída temporárias**

| Local        | Diretriz    | Funções                                |
|--------------|-------------|----------------------------------------|
| rsed.envvars | CGL_ISPWORK | Caminho inicial dos dados temporários. |
| rsed.envvars | TMPDIR      | Diretório dos dados temporários.       |

## Definições de Recursos Principais

### /etc/rdz/rsed.envvars

As variáveis de ambiente definidas em rsed.envvars são usadas por RSE, Java e z/OS UNIX. O arquivo de amostra que vem com o Developer for System z é destinado a instalações de pequeno e médio porte que não exigem os componentes opcionais do Developer for System z. "rsed.envvars, arquivo de configuração RSE"

no *Guia de Configuração do Host* (SC23-7658) descreve cada variável definida no arquivo de amostra, em que as seguintes variáveis necessitam de atenção especial:

**`_RSE_JAVA_OPTS="$_RSE_JAVA_OPTS -Xms128m -Xmx512m"`**

Defina o tamanho de heap inicial (Xms) e máximo (Xmx). Os padrões são 128M e 512M, respectivamente. Altere para aplicar os valores de tamanho de heap desejados. Se esta diretiva for removida, os valores padrão de Java serão usados, que são 4M e 512M respectivamente.

**`#_RSE_JAVA_OPTS="$_RSE_JAVA_OPTS -Dmaximum.clients=30"`**

Quantidade máxima de clientes atendidos por um conjunto de encadeamentos. O padrão é 30. Remova o comentário e customize para limitar o número de clientes por conjunto de encadeamentos. Observe que outros limites podem impedir que o RSE atinja esse limite.

**`#_RSE_JAVA_OPTS="$_RSE_JAVA_OPTS -Dmaximum.threads=520"`**

Valor máximo dos encadeamentos ativos em um conjunto de encadeamentos para permitir clientes novos. O padrão é 520. Remova o comentário e customize para limitar o número de clientes por conjunto de encadeamentos baseado no número de encadeamentos em uso. Note que cada conexão do cliente usa diversos encadeamentos (17 ou mais) e que outros limites podem evitar que o RSE atinja esse limite.

**Nota:** Esse valor deve ser inferior ao configurado para MAXTHREADS e MAXTHREADTASKS, em SYS1.PARMLIB(BPXPRMxx).

**`#_RSE_JAVA_OPTS="$_RSE_JAVA_OPTS -Dminimum.threadpool.process=1"`**

O número mínimo de conjuntos de encadeamentos ativos. O padrão é 1. Remova o comentário e customize para iniciar pelo menos o número listado de processos do conjunto de encadeamentos. Os processos do conjunto de encadeamentos são usados para balanceamento de carga dos encadeamentos do servidor RSE. Mais novos processos serão iniciados quando forem necessários. Iniciar os novos processos diretamente ajuda a evitar atrasos na conexão, mas usa mais recursos durante os tempos inativos.

**Nota:** Se a diretiva `single.logon` estiver ativa, haverá, pelo menos, 2 conjuntos de encadeamentos iniciados, mesmo se `minimum.threadpool.process` estiver definido como 1. A configuração padrão para `single.logon` no `rsed.envvars` é ativo.

**`#_RSE_JAVA_OPTS="$_RSE_JAVA_OPTS -Dmaximum.threadpool.process=100"`**

O número máximo de conjuntos de encadeamentos ativos. O padrão é 100. Remova o comentário e customize para limitar o número de processos do conjunto de encadeamentos. Os processos do conjunto de encadeamentos são usados para balanceamento de carga dos encadeamentos do servidor RSE e a limitação deles limitará a quantidade de conexões do cliente ativas.

## **SYS1.PARMLIB(BPXPRMxx)**

O RSE é um aplicativo Java, que significa que ele está ativo no ambiente z/OS UNIX. Isso promove o BPXPRMxx a se tornar um membro parmlib crucial, uma vez que ele contém os parâmetros que controlam o ambiente e os sistemas de arquivos do z/OS UNIX. O BPXPRMxx é descrito no *MVS Initialization and Tuning Reference* (SA22-7592). As seguintes diretivas são conhecidas por impactar o Developer for System z:

**MAXPROCSYS(nnnnn)**

Especifica o número máximo de processos que o sistema permite.

Intervalo de Valor: nnnnn é um valor decimal de 5 a 32767.  
Padrão: 900

#### **MAXPROCUSER(nnnnn)**

Especifica o número máximo de processos que um único ID de usuário do z/OS UNIX pode ter ativo simultaneamente, independentemente de como os processos foram criados.

Intervalo de Valor: nnnnn é um valor decimal de 3 a 32767.  
Padrão: 25

#### **Nota:**

- Todos os processos RSE usam o mesmo ID do usuário do z/OS UNIX (aquele do usuário que está designado ao daemon do RSE), pois todos os clientes são executados como encadeamentos dentro dos processos RSE.
- Esse valor pode ser definido também com a variável PROCUSERMAX no segmento de perfil de segurança OMVS do usuário designado à tarefa iniciada do RSED.

#### **MAXTHREADS(nnnnnn)**

Especifica o número máximo de encadeamentos pthread\_created, incluindo execução, enfileiramento e saída, exceto desconexão, que um único processo pode ter ativado simultaneamente. Especificar um valor de 0 impede que os aplicativos usem pthread\_create.

Intervalo de Valor: nnnnnn é um valor decimal de 0 a 100000.  
Padrão: 200

#### **Nota:**

- Cada cliente usa pelo menos 17 encadeamentos dentro do processo do conjunto de encadeamentos do RSE e vários clientes são ativados dentro do processo.
- Esse valor pode ser configurado também com a variável THREADSMAX no segmento do perfil de segurança OMVS do usuário designado à tarefa iniciada do RSED. Quando configurado, o valor THREADSMAX é usado para MAXTHREADS e MAXTHREADTASKS.

#### **MAXTHREADTASKS(nnnnn)**

Especifica o número máximo de tarefas MVS que um único processo pode ter ativado simultaneamente para encadeamentos pthread\_created.

Intervalo de Valor: nnnnn é um valor decimal de 0 a 32768.  
Padrão: 1000

#### **Nota:**

- Cada encadeamento ativo possui uma tarefa MVS (TCB, Bloco de Controle da Tarefa).
- Cada tarefa MVS simultânea exige armazenamento adicional, algumas das quais devem ficar abaixo da linha de 16 MB.
- Cada cliente usa pelo menos 17 encadeamentos dentro do processo do conjunto de encadeamentos do RSE e vários clientes são ativados dentro do processo.
- Esse valor pode ser configurado também com a variável THREADSMAX no segmento do perfil de segurança OMVS do usuário designado à tarefa

iniciada do RSED. Quando configurado, o valor THREADSMAX é usado para MAXTHREADS e MAXTHREADTASKS.

#### **MAXUIDS(nnnnn)**

Especifica o número máximo de IDs do usuário (UIDs) do z/OS UNIX que podem funcionar simultaneamente.

Intervalo de Valor: nnnnn é um valor decimal de 1 a 32767.

Padrão: 200

#### **MAXASSIZE(nnnnn)**

Especifica os valores de recursos RLIMIT\_AS que serão estabelecidos como os valores iniciais para os novos processos. RLIMIT\_AS indica o tamanho da região de espaço de endereço.

Intervalo de Valor: nnnnn é um valor decimal de 10485760 (10 Megabytes) a 2147483647 (2 Gigabytes).

Padrão: 209715200 (200 Megabytes)

#### **Nota:**

- Esse valor deve ser configurado como 2 G.
- Esse valor pode ser configurado com a variável ASSIZEMAX no segmento de perfil de segurança OMVS do usuário designado à tarefa iniciada do RSED.

#### **MAXFILEPROC(nnnnnn)**

Especifica o número máximo de descritores para arquivos, soquetes, diretórios e quaisquer outros objetos do sistema de arquivos que um único processo pode ter ativado ou alocado simultaneamente.

Intervalo de Valor: nnnnnn é um valor decimal de 3 a 524287.

Padrão: 64000

#### **Nota:**

- Um conjunto de encadeamentos possui todos os encadeamentos de clientes em um único processo.
- Esse valor pode ser configurado também com a variável FILEPROCMAX no segmento do perfil de segurança OMVS do usuário designado à tarefa iniciada do RSED.

#### **MAXMAPAREA(nnnnn)**

Especifica a quantidade máxima de espaço de armazenamento do espaço de dados (em páginas) que pode ser alocada para mapeamentos de memória de arquivos z/OS UNIX. O armazenamento não é alocado até que o mapeamento de memória esteja ativado.

Intervalo de Valor: nnnnn é um valor decimal de 1 a 16777216.

Padrão: 40960

**Nota:** Esse valor pode ser configurado também com a variável MMAPAREAMAX no segmento do perfil de segurança OMVS do usuário designado à tarefa iniciada do RSED.

Use o comando do operador **SETOMVS** ou **SET OMVS** para aumentar ou diminuir dinamicamente (até o próximo IPL) o valor de quaisquer variáveis BPXPRMxx anteriores. Para fazer uma alteração permanente, edite o membro

BPXPRMxx que será usado para IPLs. Consulte *MVS System Commands* (SA22-7627) para obter informações adicionais sobre esses comandos do operador.

As definições a seguir são subparâmetros da instrução NETWORK.

**MAXSOCKETS (nnnnnnnn)**

Especifica o número máximo de soquetes suportados por esse sistema de arquivos para essa família de endereços. Esse é um parâmetro opcional.

Intervalo de Valor: nnnnnnn é um valor decimal de 0 a 16777215.

Padrão: 100

**INADDRANYCOUNT (nnnn)**

Especifica o número de portas que o sistema reserva para uso com a PORT 0, as ligações INADDR\_ANY, começando com o número de porta especificado no parâmetro INADDRANYPORT. Esse valor é necessário apenas para CINET (várias pilhas TCP/IP).

Intervalo de Valor: nnnn é um valor decimal de 1 a 4000.

Padrão: Se nenhum INADDRANYPORT ou INADDRANYCOUNT

for especificado, o padrão para INADDRANYCOUNT será 1000.

Caso contrário, nenhuma porta será reservada (0).

---

## Várias definições de recurso

### Placa EXEC na JCL do Servidor

As definições a seguir são recomendadas a serem incluídas na placa EXEC no JCL dos servidores Developer for System z.

**REGION=0M**

REGION=0M é recomendado para o daemon RSE e as tarefas iniciadas do JES Job Monitor, RSED e JMON, respectivamente. Fazendo isso, o tamanho do espaço de endereço fica limitado apenas pelo armazenamento privado disponível, ou pelas saídas do sistema IEFUSI ou IEALIMIT. Observe que é altamente recomendado pela IBM que essas saídas não sejam usadas para espaços de endereços z/OS UNIX, como o daemon RSE.

**TIME=NOLIMIT**

TIME=NOLIMIT é recomendado a ser usado para todos os servidores Developer for System z. Isso porque o tempo de CPU de todos os clientes Developer for System z acumula nos espaços de endereço do servidor.

### FEK.#CUST.PARMLIB(FEJJCNFG)

As variáveis de ambiente definidas em FEJJCNFG são usadas pelo JES Job Monitor. O arquivo de amostra fornecido com o Developer for System z destina-se a instalações de porte médio e pequeno. "FEJJCNFG, JES Arquivo de configuração do monitor de tarefas" no *Guia de Configuração do Host* (SC23-7658) descreve cada variável definida no arquivo de amostra, em que as seguintes variáveis necessitam de atenção especial:

**MAX\_THREADS**

Número máximo de usuários que podem utilizar um Monitor de Tarefas do JES por vez. O padrão é 200. O valor máximo é 2147483647. Aumentar este número pode exigir o aumento do tamanho do espaço de endereços do JES Job Monitor.



## SYS1.PARMLIB(IEASYSxx)

IEASYSxx mantém parâmetros do sistema e é descrito no *MVS Initialization and Tuning Reference* (SA22-7592). As diretivas a seguir são conhecidas por impactar o Developer for System z:

### MAXUSER=nnnnn

Esse parâmetro especifica um valor que, na maioria das condições, o sistema usa para limitar o número de tarefas e as tarefas iniciadas que podem ser executadas simultaneamente durante um IPL específico.

Intervalo de Valor: nnnnn é um valor decimal de 0-32767. Note que os valores especificados para os parâmetros do sistema MAXUSER, RSVSTRT e RSVNONR não pode exceder 32767.

Valor-padrão: 255

## SYS1.PARMLIB(IVTPRMxx)

IVTPRMxx configura parâmetros para o Communication Storage Manager (CSM), e é descrito no *MVS Initialization and Tuning Reference* (SA22-7592). As seguintes diretivas são conhecidas por impactar o Developer for System z:

### FIXED MAX(maxfix)

Define a quantidade máxima de armazenamento dedicada a buffers fixos do CSM.

Intervalo de Valor: maxfix é um valor de 1024K a 2048M.

Padrão: 100M

### ECSA MAX(maxecsa)

Define a quantidade máxima de armazenamento dedicada a buffers do ECSA CSM.

Intervalo de Valor: maxecsa é um valor de 1024K a 2048M.

Padrão: 100M

## SYS1.PARMLIB(ASCHPMxx)

Um membro parmlib ASCHPMxx contém informações de planejamento para o planejador de transação ASCH e é descrito no *MVS Initialization and Tuning Reference* (SA22-7592). As diretivas a seguir são conhecidas por impactar o Developer for System z:

### MAX(nnnnn)

Um parâmetro opcional da definição CLASSADD que especifica o número máximo de iniciadores de transações APPC que são permitidos em uma determinada classe de iniciadores de transações. Depois que esse limite for atingido, nenhum novo espaço de endereço será criado e os pedidos recebidos serão enfileirados para aguardar até que os espaços de endereço do iniciador existentes se tornem disponíveis. O valor não deve exceder o número máximo de espaços de endereço permitido por sua instalação e você deve estar ciente dos produtos concorrentes no sistema que também exigirão espaços de endereço.

Intervalo de Valor: nnnnn é um valor decimal de 1 a 64000.

Padrão: 1



**Nota:** Se você usar APPC para iniciar o serviço TSO Commands, então a classe de transações usada deve ter iniciadores de transações suficientes para permitir um iniciador para cada usuário concorrente do Developer for System z.

## Monitoramento

Como as cargas de trabalho do usuário podem alterar a necessidade de recursos do sistema, o sistema deve ser monitorado regularmente para medir o uso de recursos de modo que o Rational Developer for System z e as configurações do sistema possam ser ajustadas em resposta aos requisitos do usuário. Os comandos a seguir podem ser usados para ajudar nesse processo de monitoramento.

### Monitoramento de RSE

Os conjuntos de encadeamentos RSE são o ponto focal para a atividade do usuário no Developer for System z e, assim, exigem monitoramento para o uso ideal. O daemon RSE pode ser consultado sobre informações que não podem ser reunidas com as ferramentas de monitoramento comuns do sistema.

- Use as ferramentas de monitoramento comuns do sistema, como RMF, para reunir dados específicos de espaço de endereço, como armazenamento real e tempo de CPU. Se você não tiver uma ferramenta de monitoramento dedicada, então as informações básicas poderão ser reunidas com ferramentas como a visualização SDSF DA ou TASID (uma ferramenta de informações do sistema como elas estão armazenadas no banco de dados disponível por meio da página da Web “Support and Downloads”).
- Durante a inicialização, o daemon RSE relata o tamanho do espaço de endereço disponível e o tamanho de heap Java com a mensagem do console FEK004I.

```
FEK004I RseDaemon: Tamanho Máximo de Heap=65MB e Tamanho do AS privado=1,959MB
```

- O comando do operador **MODIFY RSED,APPL=DISPLAY PROCESS** exibe os processos do conjunto de encadeamentos do RSE. O campo “Uso de Memória” mostra quanto do heap Java definido é realmente usado. Consulte “Comandos do operador” no *Guia de Configuração do Host* (SC23-7658) para obter informações adicionais sobre esse comando.

```
f rsed,appl=d p
BPXM023I (STCRSE)
ID do processo(16777456) Uso de Memória(33%) Clientes(4) Ordem(1)
```

Informações adicionais são fornecidas quando a opção **DETAIL** do comando de modificação do **DISPLAY PROCESS** é usado:

```
f rsed,appl=d p,detail
BPXM023I (STCRSE)
ID do processo(33555087) ASId(002E) Nome da Tarefa (RSED8) Ordem(1)
PROCESS LIMITS: CURRENT HIGHWATER LIMIT
JAVA HEAP USAGE(%) 10 56 100
CLIENTS 0 25 30
MAXFILEPROC 83 103 64000
MAXPROCUSER 97 99 200
MAXTHREADS 9 14 1500
MAXTHREADTASKS 9 14 1500
```

A opção de CPU do comando de modificação **DISPLAY PROCESS** mostrará o uso acumulado de CPU (em milissegundos) de cada encadeamento em um conjunto de encadeamentos:

```
f rsed,appl=d p,cpu
BPXM023I (STCRSE)
ID do processo(33555087) ASId(002E) Nome da Tarefa (RSED8) Ordem(1)
USERID THREAD-ID TCB# ACC_TIME TAG
STCRSE 0EDE540000000000 005E6860 822 1/ThreadPoolProcess
STCRSE 0EDE870000000001 005E69C8 001
STCRSE 0EDE980000000002 005E6518 1814
STCRSE 0EDEBA0000000003 005E66B0 2305
STCRSE 0EDECB0000000004 005E62F8 001
STCRSE 0EDED00000000005 005E60D8 001
STCRSE 0EDF860000000006 005C2BF8 628 6/ThreadPoolMonitor$Memory
UsageMonitor
STCRSE 0EDF970000000007 005C2D90 003 7/ThreadPoolMonitor
IBMUSER 0EE2C70000000024 005C08B0 050 38/JESMiner
IBMUSER 0EE2B60000000026 005C0690 004 40/FAMiner
IBMUSER 0EE30B0000000027 005C0250 002 41/LuceneMiner
IBMUSER 0EE31C0000000028 005C0030 002 42/CDTParserMiner
IBMUSER 0EE32D0000000029 005B0E00 002 43/MVSLuceneMiner
IBMUSER 0EE33E000000002A 005B0BE0 002 44/CDTMVSParserMiner
```

- Quando um processo de conjunto de encadeamentos do RSE termina, ele exibe estatísticas de uso de recursos detalhadas, como se o comando **DISPLAY PROCESS,DETAIL** modify fosse emitido para apenas esse processo de conjunto de encadeamentos do RSE. O limite máximo mostra o uso de recurso simultâneo máximo durante a vida do processo de conjunto de encadeamentos do RSE, permitindo a um ajustador de sistema determinar se os recursos designados ao RSE estão alocados acima ou abaixo do nível.

## Monitorando o z/OS UNIX

A maioria dos limites z/OS UNIX que é do interesse do Developer for System z pode ser exibida usando comandos do operador. Alguns comandos mostram ainda o uso atual e a limite máximo de um limite específico. Consulte *MVS System Commands* (SA22-7627) para obter informações adicionais sobre esses comandos.

- A diretiva LIMMSG(ALL) em SYS1.PARMLIB(BPXPRMxx) informa ao z/OS UNIX para exibir mensagens do console (BPXI040I) quando qualquer dos limites parmlib estiver prestes a ser atingido. O valor-padrão de LIMMSG é NONE, que desativa a função. Use o comando do operador **SETOMVS LIMMSG=ALL** para ativar dinamicamente essa função (até o próximo IPL). Consulte *MVS Initialization and Tuning Reference* (SA22-7592) para obter mais informações sobre esta diretiva.
- O comando do operador **DISPLAY OMVS,OPTIONS** exibe os valores atuais das diretivas z/OS UNIX que podem ser definidas dinamicamente.

```
d omvs,o
BPX0043I 13.10.16 DISPLAY OMVS 066
OMVS 0000 ETC/INIT WAIT OMVS=(M7)
CURRENT UNIX CONFIGURATION SETTINGS:
MAXPROCSYS = 256 MAXPROCUSER = 16
MAXFILEPROC = 256 MAXFILESIZE = NOLIMIT
MAXCPUPTIME = 1000 MAXUIDS = 200
MAXPTYS = 256
MAXMMAPAREA = 256 MAXASSIZE = 209715200
MAXTHREADS = 200 MAXTHREADTASKS = 1000
MAXCORESIZE = 4194304 MAXSHAREPAGES = 4096
IPCMSGQBYTES = 2147483647 IPCMSGQNUM = 10000
IPCSEMNIDS = 500 IPCSEMNIDS = 500
IPCSEMNOPS = 25 IPCSEMNSEMS = 1000
IPCSEMNPPAGES = 25600 IPCSEMNIDS = 500
IPCSEMNSEGS = 500 IPCSEMNPPAGES = 262144
SUPERUSER = BPXROOT FORKCOPY = COW
STEPLIBLIST =
USERDALIATABLE=
SERV_LINKLIB = POSIX.DYN SERV.LOADLIB BPXLK1
SERV_LPALIB = POSIX.DYN SERV.LOADLIB BPXLK1
PRIORITYPG VALUES: NONE
PRIORITYGOAL VALUES: NONE
MAXQUEUESIGS = 1000 SHRLIBRGNSIZE = 67108864
SHRLIBMAXPAGES = 4096 VERSION = /
SYSCALL COUNTS = NO TTYGROUP = TTY
SYSPLX = NO BRML SERVER = N/A
LIMMSG = NONE AUTOCVT = OFF
RESOLVER PROC = DEFAULT
AUTHPGMLIST = NONE
SWA = BELOW
```

- O comando do operador **DISPLAY OMVS,LIMITS** exibe informações sobre limites parmlib atuais dos Serviços do Sistema z/OS UNIX, seus limites máximos e o uso atual do sistema.

```
d omvs,l
BPX0051I 14.05.52 DISPLAY OMVS 904
OMVS 0042 ACTIVE OMVS=(69)
SYSTEM WIDE LIMITS: LIMMSG=SYSTEM
CURRENT HIGHWATER SYSTEM
USAGE USAGE LIMIT
MAXPROCSYS 1 4 256
MAXUIDS 0 0 200
MAXPTYS 0 0 256
MAXMMAPAREA 0 0 256
MAXSHAREPAGES 0 10 4096
IPCSEMNIDS 0 0 500
IPCSEMNIDS 0 0 500
IPCSEMNIDS 0 0 500
IPCSEMNPPAGES 0 0 262144 *
IPCMSGQBYTES --- 0 262144
IPCMSGQNUM --- 0 10000
IPCSEMNPPAGES --- 0 256
SHRLIBRGNSIZE 0 0 67108864
SHRLIBMAXPAGES 0 0 4096
```

O comando exibe limites máximos e o uso atual de um processo individual quando a palavra-chave PID=processid também for especificada.

```
d,omvs,l,pid=1677456
BPX0051I 14.06.28 DISPLAY OMVS 645
OMVS 000E ACTIVE OMVS=(76)
```

```

USER JOBNAME ASID PID PPID STATE START CT_SECS
STCRSE RSED8 007E 16777456 67109106 HF----- 20.00.56 113.914
LATCHWAITPID= 0 CMD=java -Ddaemon.log=/var/rdz/logs -
PROCESS LIMITS:
CURRENT HIGHWATER PROCESS
USAGE USAGE LIMIT

MAXFILEPROC 83 103 256
MAXFILESIZE --- --- NOLIMIT
MAXPROCUSER 97 99 200
MAXQUEUEDSIG 0 1 1000
MAXTHREADS 9 14 200
MAXTHREADTASKS 9 14 1000
IPCshmSEGS 0 0 500
MAXCORESIZE --- --- 4194304
MAXMEMLIMIT 0 0 16383P

```

- O comando do operador **DISPLAY OMVS,PFS** exibe informações sobre cada sistema de arquivo físico que faz parte atualmente da configuração do z/OS UNIX, que inclui as pilhas TCP/IP.

```

d omvs,p
BPX0046I 14.35.38 DISPLAY OMVS 092
OMVS 000E ACTIVE OMVS=(33)
PFS CONFIGURATION INFORMATION
PFS TYPE DESCRIPTION ENTRY MAXSOCK OPNSOCK HIGHUSED
TCP SOCKETS AF_INET EZBPFINI 50000 244 8146
UDS SOCKETS AF_UNIX BPXTUINI 64 6 10
ZFS LOCAL FILE SYSTEM IOEFSCM
14:32:00 RECYCLING
HFS LOCAL FILE SYSTEM GFUAINIT
BPXFTCLN CLEANUP DAEMON BPXFTCLN
BPXFTSYN SYNC DAEMON BPXFTSYN
BPXFPINT PIPE BPXFPINT
BPXFCSIN CHAR SPECIAL BPXFCSIN
NFS REMOTE FILE SYSTEM GFSCINIT
PFS NAME DESCRIPTION ENTRY STATUS FLAGS
TCP41 SOCKETS EZBPFINI ACT CD
TCP42 SOCKETS EZBPFINI ACT
TCP43 SOCKETS EZBPFINI INACT SD
TCP44 SOCKETS EZBPFINI INACT
PFS PARM INFORMATION
HFS SYNCDEFAULT(60) FIXED(50) VIRTUAL(100)
CURRENT VALUES: FIXED(55) VIRTUAL(100)
NFS bi0d(6)

```

- O comando do operador **DISPLAY OMVS,PID=processid** exibe as informações de encadeamento de um processo específico.

```

d omvs,pid=16777456
BPX0040I 15.30.01 DISPLAY OMVS 637
OMVS 000E ACTIVE OMVS=(76)
USER JOBNAME ASID PID PPID STATE START CT_SECS
STCRSE RSED8 007E 16777456 67109106 HF----- 20.00.56 113.914
LATCHWAITPID= 0 CMD=java -Ddaemon.log=/var/rdz/logs -
THREAD ID TCB0 PRI_JOB USERNAME ACC_TIME SC STATE
0E08A00000000000 005E6DFO OMVS .927 RCV FU
0E08F00000000000 005E6C58 .001 PTX JYNV
0E09300000000000 005E6AC0 7.368 PTX JYNV
0E0CB00000000000 005C2CFO OMVS 1.872 SEL JFNV
0E1920000000003CE 005A0B70 OMVS 14.088 POL JFNV
0E18D0000000003CF 005A1938 IBMUSER .581 SND JYNV

```

## Monitoramento da Rede

Ao suportar um grande número de clientes se conectando ao host, não só o Developer for System z, mas também sua infraestrutura de rede deve poder manipular a carga de trabalho. O gerenciamento de redes é um assunto amplo e bem documentado que sai do escopo da documentação do Developer for System z. Portanto, apenas os seguintes ponteiros são fornecidos.

- O comando do operador **DISPLAY NET,CSM** permite que você monitore o uso de armazenamento gerenciado pelo gerenciador de armazenamento de comunicações (CSM). Você pode usar esse comando para determinar a quantidade de armazenamento do CSM que está em uso no ECSA e os conjuntos de armazenamento de espaço de dados, conforme documentado em *Communications Server SNA Operations* (SC31-8779).

## Monitorando Sistemas de Arquivos z/OS UNIX

Developer for System z usa sistemas de arquivo z/OS UNIX para armazenar vários tipos de dados, como arquivos de logs e temporários. Use o comando z/OS UNIX **df** para verificar quantos descritores de arquivo ainda estão disponíveis e quanto espaço livre foi deixado antes que a próxima extensão do conjunto de dados subjacente HFS ou zFS seja criada.

```
$ df
Mounted on Filesystem Avail/Total Files Status
/tmp (OMVS.TMP) 1393432/1396800 4294967248 Available
/u/ibmuser (OMVS.U.IBMUSER) 1248/1728 4294967281 Available
/usr/lpp/rdz (OMVS.LPP.FEK) 3062/43200 4294967147 Available
/var (OMVS.VAR) 27264/31680 4294967054 Available
```

## Configuração de Amostra

A configuração de amostra a seguir mostra a configuração necessária para suportar estes requisitos:

- 500 conexões do cliente simultâneas
- 300 builds MVS simultâneos (tarefa em lote)
- 200 conexões CARMA simultâneas (usando o método de inicialização CRASTART)
- tempo limite de inatividade de 3 horas
- uso não autorizado de z/OS UNIX
- O SCLM Developer Toolkit não é usado
- Calcule uma média de uso de heap Java de 20 MB
- os usuários têm UIDs z/OS UNIX exclusivos
- Os conjuntos de encadeamentos operam no modo de minerador multiencadeado

## Contagem do Conjunto de Encadeamento

Por padrão, o Developer for System z tenta incluir 30 usuários em um conjunto de encadeamentos únicos. Entretanto, nossos requisitos indicam que o tempo limite de inatividade estará ativo. A Tabela 29 na página 86 mostra que isso incluirá 1 encadeamento por cliente conectado. Esse encadeamento é um encadeamento de cronômetro e portanto ativo constantemente. Isso evitará que o RSE coloque 30 usuários em um único conjunto de encadeamentos, como  $10 + 30 \times (17 + 1) = 550$ , e `maximum.threads` é configurado para 520 por padrão.

Poderíamos aumentar `maximum.threads`, mas devido ao requisito ter uma média de 20 MB de heap Java por usuário, optamos por diminuir o `maximum.clients` para 25 ( $10 + 25 \times 18 = 460$ ). Isso nos mantém dentro do tamanho máximo padrão de heap Java de 512 MB ( $20 \times 25 = 500$ ).

Com 25 clientes por conjunto de encadeamentos e a necessidade de suportar 500 conexões, sabemos agora que precisaremos de 20 espaços de endereço de conjunto de encadeamentos.

## Determinar Limites Mínimos

Usando as fórmulas mostradas anteriormente neste capítulo e os critérios mencionados no início desta seção, podemos determinar o uso do recurso que deve ser adaptado.

- Contagem de espaço de endereço - máximo  
 $3 + 2 \times A + N \times (x + y + z) + (2 + N \times 0.01)$   
 $3 + 2 \times 20 + 500 \times 1 + 200 \times 1 + 300 \times 1 + (2 + 500 \times 0.01) = 1050$
- Contagem de espaço de endereço - por usuário  
 $x + y + z$   
 $1 + 1 + 1 = 3$
- Contagem de processos - máximo  
 $6 + 3 \times A + N \times (x + y + z) + (10 + N \times 0.05)$   
 $6 + 3 \times 20 + 500 \times 2 + 200 \times 1 + 300 \times 0 + (10 + 500 \times 0.05) = 1591$

- Contagem de processo - STCRSE  
 $4 + 3 \cdot A$   
 $4 + 3 \cdot 20 = 64$
- Contagem de processos - por usuário  
 $(x + y + z) + 5 \cdot s$   
 $(2 + 1 + 0) + 5 \cdot 0 = 3$
- Contagem de encadeamentos - Conjunto de encadeamentos do RSE  
 $12 + N \cdot (19 + x + y + z) + (20 + N \cdot 0.1)$   
 $12 + 25 \cdot (19 + 1 + 4 + 0) + (20 + 25 \cdot 0.1) = 635$
- Contagem de encadeamentos - JES Job Monitor  
 $3 + N + (20 + N \cdot 0.1)$   
 $3 + 500 + (20 + 500 \cdot 0.1) = 573$
- Contagem de encadeamentos - Debug Manager  
 $4$   
 $4$
- IDs do Usuário  
 $500 + 3 = 503$   
 Os 3 IDs do usuário extra são para STCJMON, STCDBM, e STCRSE, os IDs do usuário da tarefa iniciada Developer for System z.

## Definindo Limites

Agora que os números de uso de recursos são conhecidos, podemos customizar a limitação das diretivas com valores apropriados.

- /etc/rdz/rsed.envvars
  - Xmx512m  
  
não alterado
  - Dmaximum.clients=25
  - Dmaximum.threads=520  
  
não alterado
  - Dminimum.threadpool.process=10  
 Esta mudança é opcional; o RSE iniciará novos conjuntos de encadeamentos, conforme necessário
  - DDSTORE\_USE\_THREADED\_MINERS=true
  - DHIDE\_ZOS\_UNIX=true
  - DDSTORE\_IDLE\_SHUTDOWN\_TIMEOUT=10800000
- FEK.#CUST.PARMLIB(FEJJCNFG)
  - MAX\_THREADS=573
- SYS1.PARMLIB(BPXPRMxx)
  - MAXPROCSYS(2500)  
  
1591 mínimo, incluído buffer extra para tarefas diferentes de Developer for System z
  - MAXPROCUSER(100)

64 mínimo, incluído buffer extra no caso de conjuntos de os encadeamentos do RSE suportarem menos que os 25 clientes projetados

- MAXTHREADS(1500)

deve ter no mínimo 573 (para o JES Job Monitor) se THREADSMAX no segmento OMVS do ID do usuário STCRSE for usado para configurar o limite para RS (mínimo de 635)

- MAXTHREADTASKS(1500)

devem ter no mínimo 573 (para o JES Job Monitor) se THREADSMAX no segmento OMVS do ID do usuário STCRSE for usado para configurar o limite para RS (mínimo de 635)

- MAXUIDS(700)

503 mínimo, incluído buffer extra para tarefas que não  
Developer  
for System z

- MAXASSIZE(209715200)

não alterado (padrão do sistema 200 MB), usamos ASSIZEMAX no segmento OMVS do ID do usuário STCRSE

- SYS1.PARMLIB(IEASYSxx)
  - MAXUSER=2000

1050 mínimo, incluído buffer extra para tarefas diferentes de  
Developer  
for System z

- Segmento OMVS do ID do usuário STCRSE
  - ASSIZEMAX(2147483647)

2 GB

## Uso de Recurso de Monitor

Após ativar os limites do sistema conforme documentado em “Definindo Limites” na página 110, podemos começar a monitorar o uso do recurso pelo Developer for System z para ver se o ajuste de algumas variáveis é necessário. O Figura 31 na página 112 mostra o uso de recurso após 499 usuários terem efetuado logon. (O exemplo na figura apenas mostra a criação do logon. Nenhuma ação do usuário é indicada no exemplo).

```

F RSED,APPL=D P
BPXM023I (STCRSE)
ProcessId(83886168) Memory Usage(17%) Clients(25) Order(1)
ProcessId(91) Memory Usage(17%) Clients(25) Order(2)
ProcessId(122) Memory Usage(17%) Clients(25) Order(3)
ProcessId(16777348) Memory Usage(17%) Clients(25) Order(4)
ProcessId(16777358) Memory Usage(17%) Clients(25) Order(5)
ProcessId(16777368) Memory Usage(17%) Clients(25) Order(6)
ProcessId(16777378) Memory Usage(17%) Clients(25) Order(7)
ProcessId(16777388) Memory Usage(17%) Clients(25) Order(8)
ProcessId(16777398) Memory Usage(17%) Clients(25) Order(9)
ProcessId(33554622) Memory Usage(17%) Clients(25) Order(10)
ProcessId(16777416) Memory Usage(17%) Clients(25) Order(11)
ProcessId(16777426) Memory Usage(17%) Clients(25) Order(12)
ProcessId(16777436) Memory Usage(9%) Clients(25) Order(13)
ProcessId(16777446) Memory Usage(17%) Clients(25) Order(14)
ProcessId(16777456) Memory Usage(17%) Clients(25) Order(15)
ProcessId(16777466) Memory Usage(17%) Clients(25) Order(16)
ProcessId(16777476) Memory Usage(17%) Clients(25) Order(17)
ProcessId(16777487) Memory Usage(17%) Clients(25) Order(18)
ProcessId(16777497) Memory Usage(17%) Clients(25) Order(19)
ProcessId(16777507) Memory Usage(16%) Clients(24) Order(20)

F RSED,APPL=D P,D
BPXM023I (STCRSE)
ProcessId(83886168) ASId(0022) JobName(RSED857) Order(1)
PROCESS LIMITS: CURRENT HIGHWATER LIMIT
JAVA HEAP USAGE(%) 17 17 100
CLIENTS 25 25 25
MAXFILEPROC 365 366 64000
MAXPROCUSE 64 64 100
MAXTHREADS 362 363 1500
MAXTHREADTASKS 363 363 1500

TASID
Nome Tarefa Tempo de CPU Armazen. EXCP

JMON 0.00 1780 73
RSED 5.88 95.2M 41958
RSED1 8.26 190.1M 58669
RSED1 8.17 187.0M 58605
RSED2 8.06 185.3M 58653
RSED2 8.19 183.1M 60209
RSED3 8.12 189.1M 58650
RSED3 8.03 186.7M 58590
RSED4 8.15 188.2M 58646
RSED4 5.50 182.5M 58585
RSED5 7.72 184.4M 58631
RSED5 7.82 184.1M 58576
RSED6 7.14 184.1M 58622
RSED6 6.27 186.9M 58583
RSED7 5.17 185.1M 58804
RSED7 6.57 185.2M 58621
RSED7 5.86 182.8M 58565
RSED8 0.36 1560 2459
RSED8 7.94 184.1M 58615
RSED8 7.45 181.8M 58548
RSED9 8.16 190.6M 58802
RSED9 7.62 183.8M 58610
RSED9 7.36 177.7M 57478

```

Figura 31. Uso do recurso de configuração de amostra

---

## Capítulo 6. Considerações sobre Desempenho

O z/OS é um sistema operacional altamente customizável, e (algumas vezes pequenas) alterações no sistema podem ter um grande impacto sobre o desempenho geral. Este capítulo destaca algumas alterações que podem ser feitas para aprimorar o desempenho do Developer for System z.

Consulte *MVS Initialization and Tuning Guide* (SA22-7591) e *UNIX System Services Planning* (GA22-7800) para obter informações adicionais sobre o ajuste do sistema.

---

### Usar Sistemas de Arquivos zFS

O zFS (zSeries File System) e o HFS (Hierarchical File System) são sistemas de arquivo UNIX que podem ser usados em um ambiente z/OS UNIX. No entanto, o zFS fornece os seguintes recursos e benefícios:

- Ganhos de desempenho em vários ambientes do cliente ao acessar arquivos com tamanhos aproximados a 8 K, frequentemente acessados e atualizados. O desempenho do acesso de arquivos menores equivale àquele do HFS.
- Clonagem de leitura de um sistema de arquivo no mesmo conjunto de dados. O sistema de arquivo clonado pode ser disponibilizado aos usuários para fornecer uma cópia de leitura em um determinado momento de um sistema de arquivo. Esse é um recurso opcional disponível apenas em um ambiente não sysplex.
- O zFS é o sistema de arquivo z/OS UNIX estratégico. A funcionalidade do HFS foi estabilizada e os aprimoramentos no sistema de arquivo ocorrerão apenas para o zFS.

Consulte *UNIX System Services Planning* (GA22-7800) para saber mais sobre zFS.

---

### Evite o Uso de STEPLIB

Cada processo do z/OS UNIX que possui um STEPLIB que é propagado de pai para filho ou através de um exec consumirá cerca de 200 bytes de Extended Common Storage Area (ECSA). Se nenhuma variável de ambiente STEPLIB estiver definida, ou quando uma for definida como STEPLIB=CURRENT, o z/OS UNIX propagará todas as alocações TASKLIB, STEPLIB e JOBLIB atualmente ativas durante uma função fork(), spawn() ou exec().

O Developer for System z possui um padrão de arquivo de configuração STEPLIB=NONE codificado em `rzed.envvars`, conforme descrito em `rzed.envvars`. Pelas razões mencionadas anteriormente, não altere essa diretiva e coloque os conjuntos de dados de destino em LINKLIST ou LPA (Link Pack Area).

---

### Aprimorar o acesso às bibliotecas do sistema

Determinadas bibliotecas do sistema e módulos de carregamento são intensamente usadas pelo z/OS UNIX e pelas atividades de desenvolvimento do aplicativo. O aprimoramento do acesso, como a inclusão na Área do Pacote de Links (LPA) pode aprimorar o desempenho do sistema. Consulte *MVS Initialization and Tuning Reference* (SA22-7592) para obter informações adicionais sobre a alteração de membros SYS1.PARMLIB descrito a seguir:



## Bibliotecas de Tempo de Execução Language Environment (LE)

Quando programas C (incluindo o shell do z/OS UNIX) são executados, frequentemente usam rotinas da biblioteca de tempo de execução do LE (Language Environment). Em média, aproximadamente 4 MB da biblioteca de tempo de execução são carregados na memória para cada espaço de endereço executando um programa ativado para LE e copiados em cada fork.

CEE.SCEELPA

O conjunto de dados CEE.SCEELPA contém um subconjunto das rotinas de tempo de execução do LE, intensamente usadas pelo z/OS UNIX. Você deve incluir esse conjunto de dados em SYS1.PARMLIB(LPALSTxx) para ganho máximo de desempenho. Fazendo isso, os módulos são lidos do disco apenas uma vez e são armazenados em um local compartilhado.

**Nota:** Inclua a seguinte instrução em SYS1.PARMLIB(PROGxx), se você preferir incluir os módulos de carregamento na LPA dinâmica:

```
LPA ADD MASK(*) DSN(CEE.SCEELPA)
```

Também é aconselhável colocar as bibliotecas de tempo de execução do LE CEE.SCEERUN e CEE.SCEERUN2 em LINKLIST, incluindo os conjuntos de dados em SYS1.PARMLIB(LNKLISTxx) ou SYS1.PARMLIB(PROGxx). Isso elimina o código extra STEPLIB do z/OS UNIX e há uma redução de entrada/saída devido ao gerenciamento pelo LLA e VLF, ou produtos semelhantes.

**Nota:** Inclua a biblioteca de classes C/C++ DLL CBC.SCLBDLL também em LINKLIST pelos mesmos motivos.

Se você decidir não colocar essas bibliotecas em LINKLIST, será necessário configurar a instrução STEPLIB apropriada no arquivo de configuração rsed.envvars, conforme descrito em rsed.envvars. Embora esse método sempre utilize armazenamento virtual adicional, pode aprimorar o desempenho definindo as bibliotecas de tempo de execução do LE para o LLA ou um produto semelhante. Isso reduz a E/S necessária para carregar os módulos.

## Desenvolvimento de Aplicativos

Em sistemas em que o desenvolvimento de aplicativos é a principal atividade, o desempenho também pode ser beneficiado se você colocar o editor de ligação em um LPA dinâmico, incluindo as seguintes linhas em SYS1.PARMLIB(PROGxx):

```
LPA ADD MODNAME(CEEBINIT,CEEIBM,CEEV003,EDCV) DSN(CEE.SCEERUN)
LPA ADD MODNAME(IEFIB600,IEFXB603) DSN(SYS1.LINKLIB)
```

Para desenvolvimento do C/C++, você também pode incluir o conjunto de dados do compilador CBC.SCCNCMP em SYS1.PARMLIB(LPALSTxx).

As instruções anteriores são amostras de possíveis candidatos de LPA, mas as necessidades no seu site podem variar. Consulte *Language Environment Customization* (SA22-7564) para obter informações sobre a colocação de outros módulos de carregamento do LE na LPA dinâmica. Consulte *UNIX System Services Planning* (GA22-7800) para obter informações adicionais sobre a colocação de módulos de carregamento do compilador C/C++ em um LPA dinâmico.

---

## Aprimorando o desempenho da verificação de segurança

Para aprimorar o desempenho da verificação de segurança realizada para o z/OS UNIX, defina o perfil BPX.SAFFASTPATH na classe FACILITY do software de segurança. Isso reduz o código extra ao realizar verificações de segurança do z/OS UNIX para uma ampla variedade de operações, incluindo verificação de acesso ao arquivo, verificação de acesso ao IPC e verificação de propriedade do processo. Consulte *UNIX System Services Planning* (GA22-7800) para obter informações adicionais sobre esse perfil.

**Nota:** Os usuários não precisam ter permissão para o perfil BPX.SAFFASTPATH.

---

## Gerenciamento de carga de trabalho

Cada site possui necessidades específicas e é possível customizar o sistema operacional z/OS para aproveitar ao máximo os recursos disponíveis de acordo com essas necessidades. Com gerenciamento de carga de trabalho, você define suas metas de desempenho e designa uma importância de negócios a cada meta. Você define as metas para o trabalho em termos de negócios e o sistema decide quantos recursos, como CPU e armazenamento, devem ser fornecidos para o trabalho, de acordo com a meta.

O desempenho do Developer for System z pode ser equilibrado pela configuração das metas corretas para os processos. Algumas diretrizes gerais são listadas abaixo:

- Quando usado, designe a transação APPC para um grupo de desempenho do TSO.
- Designe um grupo de desempenho de tarefa iniciada (SYSSTC) aos espaços de endereço do servidor Developer for System z: JES Job Monitor (JMON), daemon RSE (RSED) e conjuntos de encadeamentos RSE (RSEDx).

Consulte o *MVS Planning Workload Management* (SA22-7602) para obter mais informações sobre esse assunto.

---

## Tamanho de heap Java fixo

Com um heap de tamanho fixo, nenhuma expansão ou contração de heap ocorre e isso pode ocasionar significantes ganhos de desempenho em algumas situações. No entanto, a utilização de um heap de tamanho fixo geralmente não é uma boa ideia, porque atrasa o início de uma coleta de lixo até que o heap esteja cheio, momento em que será uma tarefa principal. Também aumenta o risco de fragmentação, o que requer uma compactação de heap. Portanto, utilize heaps de tamanho fixo só depois de desempenhar teste adequado ou quando orientado pelo IBM Support Center. Consulte *Java Diagnostics Guide* (SC34-6650) para obter informações adicionais sobre tamanhos de heap e coleta de lixo.

O tamanho de heap inicial e máximo de um z/OS Java Virtual Machine (JVM) pode ser configurado com as opções da linha de comandos Java, `-Xms` (inicial) e `-Xmx` (máximo).

No Developer for System z, as opções de linha de comandos Java são definidas na diretiva `_RSE_JAVAOPTS` de `rsed.envvars`, conforme descrito em "Definindo parâmetros de inicialização Java com `_RSE_JAVAOPTS`" no *Guia de Configuração do Host* (SC23-7658).

```
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Xms128m -Xmx128m"
```

---

## Opção Java -Xquickstart

**Nota:** -Xquickstart Java é útil apenas se você utilizar o método de inicialização alternativo REXEC/SSH para o servidor RSE. Este método está documentado em "(Opcional) Usando REXEC (ou SSH)" no *Guia de Configuração do Host* (SC23-7658).

A opção -Xquickstart pode ser usada para melhorar o tempo de inicialização de alguns aplicativos Java. -Xquickstart faz com que o compilador Just In Time (JIT) seja executado com um subconjunto de otimizações, ou seja, uma compilação rápida. Essa compilação rápida permite melhorar o tempo de inicialização.

A opção -Xquickstart é apropriada para aplicativos de execução mais curta, principalmente aqueles em que o tempo de execução não está concentrado em um número pequeno de métodos. -Xquickstart pode prejudicar o desempenho se for usada em aplicativos de longa execução que contêm métodos ativos.

Para ativar a opção -Xquickstart para o servidor RSE, inclua a seguinte diretiva no final de `rsed.envvars`:

```
_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Xquickstart"
```

---

## Compartilhamento de Classe entre JVMs

O IBM Java Virtual Machine (JVM) versão 5 e superior permite compartilhar classes de aplicativos e de autoinicialização entre JVMs armazenando-as em um cache em memória compartilhada. O compartilhamento de classes reduz o consumo total de memória virtual quando mais de uma JVM compartilha um cache. O compartilhamento de classes também reduz o tempo de inicialização de uma JVM após o cache ser criado.

O cache de classe compartilhada é independente de qualquer JVM ativa e persiste além do tempo de vida da JVM que criou o cache. Como o cache de classe compartilhada persiste além do tempo de vida de qualquer JVM, o cache é atualizado dinamicamente para refletir quaisquer modificações que possam ter sido feitas em JARs ou classes no sistema de arquivo.

A sobrecarga para criar e preencher um novo cache é mínima. O custo de tempo de inicialização da JVM para uma única JVM normalmente é entre 0 e 5% menor em comparação com um sistema que não utiliza compartilhamento de classe, dependendo de quantas classes são carregadas. O aprimoramento do tempo de inicialização da JVM com um cache preenchido normalmente é entre 10% e 40% mais rápido em comparação com um sistema que não utiliza compartilhamento de classe, dependendo do sistema operacional e do número de classes carregadas. Várias JVMs em execução simultaneamente mostram maiores benefícios no tempo de inicialização total.

Consulte o *Java SDK and Runtime Environment User Guide* para obter informações adicionais sobre o compartilhamento de classe.

## Ativar Compartilhamento de Classes

Para ativar o compartilhamento de classes para o servidor RSE, inclua a seguinte diretiva no final de `rsed.envvars`. A primeira instrução define um cache denominado RSE com acesso em grupo e permite que o servidor RSE seja iniciado, mesmo se o compartilhamento de classes falhar. A segunda instrução é opcional e

configura o tamanho do cache para 6 megabytes (o padrão do sistema é 16 MB). A terceira instrução inclui os parâmetros de compartilhamento de classes nas opções de inicialização Java.

```
_RSE_CLASS_OPTS=-Xshareclasses:name=RSE,groupAccess,nonFatal
#_RSE_CLASS_OPTS="$_RSE_CLASS_OPTS -Xscmx6m
_RSE_JAVAOPTS="$_RSE_JAVAOPTS $_RSE_CLASS_OPTS"
```

**Nota:** Conforme mencionado em “Segurança do Cache”, todos os usuários que usam a classe compartilhada devem ter o mesmo ID do grupo (GID) primário. Isso significa que os usuários devem ter o mesmo grupo padrão definido no software de segurança, ou que os grupos padrão diferentes tenham o mesmo GID em seu segmento OMVS.

## Limites de Tamanho de Cache

O tamanho máximo de cache compartilhado teórico é 2 GB. O tamanho de cache que você pode especificar é limitado pela quantidade de memória física e pelo espaço de troca disponíveis para o sistema. Como o espaço de endereço virtual de um processo é compartilhado entre o cache de classe compartilhada e o heap Java, o aumento do tamanho máximo do heap Java reduzirá o tamanho do cache da classe compartilhada que você pode criar.

## Segurança do Cache

O acesso ao cache de classe compartilhada é limitado por permissões do sistema operacional e permissões de segurança Java.

Por padrão, os caches de classe são criados com a segurança no nível do usuário, portanto, apenas o usuário que criou o cache pode acessá-lo. No z/OS UNIX, há uma opção, `groupAccess`, que fornece acesso a todos os usuários no grupo primário do usuário que criou o cache. Entretanto, independentemente do nível de acesso usado, um cache poderá ser destruído apenas pelo usuário que o criou ou por um usuário root (UID 0).

Consulte o *Java SDK and Runtime Environment User Guide* para obter informações adicionais sobre as opções extras de segurança utilizando um Java SecurityManager.

## SYS1.PARMLIB(BPXPRMxx)

Algumas das configurações de SYS1.PARMLIB(BPXPRMxx) afetam o desempenho das classes compartilhadas. O uso de configurações incorretas pode interromper o funcionamento de classes compartilhadas. Essas configurações também podem ter implicações no desempenho. Para obter informações adicionais sobre implicações no desempenho e sobre o uso desses parâmetros, consulte *MVS Initialization and Tuning Reference* (SA22-7592) e *UNIX System Services Planning* (GA22-7800). Os parâmetros BPXPRMxx mais significativos que afetam a operação de classes compartilhadas são os seguintes:

- MAXSHAREPAGES, IPCSHMPAGES, IPCSHMMPAGES e IPCSHMNSEGS

Essas configurações afetam a quantidade de páginas de memória compartilhada disponíveis para a JVM. O tamanho da página compartilhada para um serviço do sistema z/OS UNIX de 31 bits é fixado em 4 KB. As classes compartilhadas tentam criar um cache de 16 MB por padrão. Entretanto, configure IPCSHMMPAGES para maior que 4096.

Se você configurar um tamanho de cache utilizando `-Xscmx`, a JVM arredondará o valor para o megabyte mais próximo. Você deve levar isso em consideração ao definir IPCSHMMPAGES no sistema.

- IPCSEMNIIDS e IPCSEMNSEMS

Essas configurações afetam a quantidade de semáforos disponíveis para os processos UNIX. As classes compartilhadas usam semáforos IPC para a comunicação entre as JVMs.

## Espaço em disco

O cache de classe compartilhada requer espaço em disco para armazenar informações de identificação sobre os caches que existem no sistema. Essas informações são armazenadas em `/tmp/javasharedresources`. Se o diretório de informações de identificação for excluído, a JVM não poderá identificar as classes compartilhadas no sistema e deverá recriar o cache.

## Utilitários de Gerenciamento de Cache

O comando da linha Java `-Xshareclasses` pode utilizar diversas opções, sendo alguns utilitários de gerenciamento do cache. Alguns deles são mostrados no exemplo a seguir (\$ é o prompt do z/OS UNIX). Consulte o *Java SDK and Runtime Environment User Guide* para obter uma visão geral completa das opções de linha de comandos suportadas.

```
$ java -Xshareclasses:listAllCaches
Shared Cache OS shmid in use Last detach time
RSE 401412 0 Mon Jun 18 17:23:16 2007

Could not create the Java virtual machine.

$ java -Xshareclasses:name=RSE,printStats

Current statistics for cache "RSE":

base address = 0x0F300058
end address = 0x0F8FFFF8
allocation pointer = 0x0F4D2E28

cache size = 6291368
free bytes = 4355696
ROMClass bytes = 1912272
Metadata bytes = 23400
Metadata % used = 1%

ROMClasses = 475
Classpaths = 4
URLs = 0
Tokens = 0
Stale classes = 0
% Stale classes = 0%

Cache is 30% full

Could not create the Java virtual machine.

$ java -Xshareclasses:name=RSE,destroy
JVMSHRC010I Shared Cache "RSE" is destroyed
Could not create the Java virtual machine.
```

### Nota:

- Os utilitários de cache executam a operação necessária no cache especificado sem iniciar a JVM, por isso a mensagem "Could not create the Java virtual machine" é normal.
- Um cache pode ser destruído apenas se todas as JVMs que o utilizam estiverem encerradas e o usuário que emite o comando tiver permissões suficientes.

---

## Capítulo 7. Considerações de Push-to-client

Push-to-client, ou controle de cliente baseado em host, suporta gerenciamento central das seguintes coisas:

- Arquivos de configuração do cliente
- Versão de produto do cliente
- Definições de projeto

Os seguintes tópicos são abordados neste capítulo:

- “Introdução”
- “Sistema Primário” na página 120
- “Metadados Push-to-client” na página 120
- “Controle de Configuração do Cliente” na página 122
- “Controle de Versão do Cliente” na página 123
- “Diversos Grupos de Desenvolvedores” na página 123
- “Seleção de Grupo Baseada em LDAP” na página 127
- “Seleção de Grupo Baseada em SAF” na página 132
- “Projetos baseados no host” na página 135

---

### Introdução

Os clientes do Developer for System z versão 8.0.1 e superior podem extrair arquivos de configuração do cliente e informações de atualização do produto do host quando eles se conectam, assegurando que todos os clientes tenham configurações comuns e estejam atualizados.

Desde a versão 8.0.3, o administrador de cliente pode criar diversos conjuntos de configuração de cliente e diversos cenários de atualização de cliente para ajustar as necessidades de diferentes grupos de desenvolvedores. Isso permite que os usuários recebam uma configuração customizada, com base em critérios como associação de um grupo LDAP ou permissão para um perfil de segurança.

Os projetos do z/OS podem ser definidos individualmente por meio da perspectiva Projetos do z/OS no cliente, ou podem ser definidos centralmente no host e propagados para o cliente em uma base por usuário individual. Esses "projetos baseados em host" se parecem e funcionam exatamente como projetos definidos no cliente, exceto que sua estrutura, seus membros e suas propriedades não podem ser modificados pelo cliente e só podem ser acessados quando conectados ao host.

`pushtoclient.properties` informa ao cliente se essas funções estão ativadas e onde os dados relacionados são armazenados. Consulte “(Opcional) `pushtoclient.properties`, Controle de Cliente Baseado em Host” no *Guia de Configuração do Host* (S517-9094) para obter mais informações.

Normalmente, os sistemas z/OS, as estações de trabalho do desenvolvedor e os projetos de desenvolvimento são gerenciados por diferentes grupos de pessoas. O design push-to-client segue esse princípio e designa responsabilidades específicas a cada grupo:

- O programador de sistema do z/OS controla o local dos metadados push-to-client, os aspectos de segurança básicos e se o push-to-client está ativo.
- O administrador de cliente mantém o conteúdo dos metadados push-to-client usando o cliente do Developer for System z para criar uma ou mais configurações de cliente e usando o IBM Installation Manager para criar os arquivos de resposta usados para atualizar o cliente do Developer for System z.
- Um gerente de projeto de desenvolvimento define um projeto e designa desenvolvedores individuais a ele.

Consulte o Centro de Informações do Developer for System z ([http://www-01.ibm.com/support/knowledgecenter/SSQ2R2\\_9.1.0/com.ibm.etools.getstart.wsentdev.doc/kc\\_version\\_welcome\\_rdz.html](http://www-01.ibm.com/support/knowledgecenter/SSQ2R2_9.1.0/com.ibm.etools.getstart.wsentdev.doc/kc_version_welcome_rdz.html)) para obter detalhes sobre como o administrador de clientes e o gerente de projetos de desenvolvimento podem executar as tarefas designadas a eles.

Ao ativar o suporte de configuração ou controle de versão para diversos grupos de desenvolvedor, uma equipe adicional será envolvida no gerenciamento de push-to-client. Qual é essa equipe depende da opção escolhida para identificar os grupos aos quais um desenvolvedor pertence:

- Um administrador de LDAP mantém as definições de grupo que colocam cada desenvolvedor em nenhum, um ou mais grupos LDAP FEK.PTC.\*.
- Um administrador de segurança mantém listas de acesso para perfis de segurança FEK.PTC.\*. Um desenvolvedor pode ser autorizado para nenhum, um ou mais perfis.

---

## Sistema Primário

O push-to-client é designado para armazenar dados específicos do sistema por sistema, enquanto mantém dados comuns (globais) em um único sistema (o sistema primário) para reduzir o esforço de gerenciamento. O sistema primário é identificado pela diretiva `primary.system` em `pushtoclient.properties`. O padrão é `false`.

Certifique-se de ter um, e apenas um, sistema definido como primário. Os administradores de cliente do Developer for System z não podem exportar dados de configuração globais, a menos que o sistema de destino seja um sistema primário. Os clientes do Developer for System z podem mostrar comportamento incorreto ao conectar-se a diversos sistemas primários com configurações fora de sincronização.

A regra somente um não se aplica quando diversos sistemas compartilham a configuração (`/etc/rdz`) e os metadados push-to-client (`/var/rdz/pushtoclient`) do Developer for System z. Como a configuração é compartilhada, todos os sistemas envolvidos são identificados como sistema primário. Mas, desde que todos os sistemas também compartilhem os metadados, essa duplicação não é um problema.

---

## Metadados Push-to-client

### Local de Metadados

A diretiva `pushtoclient.folder` em `pushtoclient.properties` identifica o diretório base no qual os metadados direcionar ao cliente são armazenados. O padrão é `/var/rdz/pushtoclient`.



O diretório base contém o arquivo de configuração push-to-client raiz, `keymapping.xml`. Todos os demais metadados estão em subdiretórios.

Em sua maioria, os subdiretórios são criados dinamicamente quando o administrador de cliente exporta a configuração da área de trabalho push-to-client. Esses subdiretórios agrupam os metadados por assunto, como mapeamentos e referências. Quanto mais componentes do cliente do Developer for System z se tornam elegíveis para serem gerenciados por direcionar ao cliente, mais subdiretórios são criados dinamicamente. Consulte o assistente de exportação no cliente do Developer for System z (**Arquivo > Exportar... > Rational Developer for System z > Arquivos de Configuração**) para saber o que é armazenado nestes subdiretórios.

Alguns subdiretórios são criados durante a customização do host inicial. Esses subdiretórios contêm dados que são mantidos manualmente pelo administrador de cliente ou pelo gerente de projeto de desenvolvimento.

- `/var/rdz/pushtoclient/projects/` mantém os arquivos de definição do projeto baseados em host. O local real é especificado em `/var/rdz/pushtoclient/keymapping.xml`, que é criado e mantido por um administrador de cliente do Developer for System z. Os arquivos contidos são mantidos por um gerenciador de projetos ou pelo desenvolvedor principal.
- `/var/rdz/pushtoclient/install/` contém os arquivos de configuração usados para atualizar a versão do produto de cliente na conexão com o host. O local real é especificado em `/var/rdz/pushtoclient/keymapping.xml`, que é criado e mantido por um administrador de cliente do Developer for System z. Os arquivos contidos são mantidos por um administrador de cliente do .
- `/var/rdz/pushtoclient/install/responsefiles/` contém os arquivos de configuração usados para atualizar a versão do produto de cliente na conexão com o host. O local real é especificado em `/var/rdz/pushtoclient/keymapping.xml`, que é criado e mantido por um administrador de cliente do Developer for System z. Os arquivos contidos são mantidos por um administrador de cliente do .

Consulte "Configuração de Customização" no capítulo "Customização Básica" do *Guia de Configuração do Host* (S517-9094) para obter mais informações sobre como a criação desses subdiretórios.

## Segurança de Metadados

Por padrão (consulte a diretiva `file.permission` em `pushtoclient.properties`), todos os arquivos e diretórios criados no diretório base recebem a máscara de bits de permissão 775 (`rw-rw-r-x`), que permite ao proprietário e ao grupo padrão do proprietário acesso de leitura e gravação à estrutura de diretório e aos arquivos contidos nela. Qualquer outra pessoa só tem acesso de leitura à estrutura de diretório e aos arquivos contidos nela.

É importante que o UID (ID do usuário) e o GID (ID do grupo) corretos do proprietário sejam configurados para esses diretórios antes de iniciar a configuração push-to-client.

Os seguintes comandos de amostra do RACF criam um novo grupo (RDZADMIN), designa a ele um GID exclusivo (2) e o torna o grupo padrão para o ID de usuário RDZADM1, que também recebe um UID exclusivo (6).

```
ADDGROUP RDZADMIN OWNER(IBMUSER) SUPGROUP(SYS1) -
 DATA('RATIONAL DEVELOPER FOR SYSTEM Z - CLIENT ADMIN')
ALTGROUP RDZADMIN OMVS(GID(2))
CONNECT RDZADM1 GROUP(RDZADMIN) AUTH(USE)
ALTUSER RDZADM1 DFLTGRP(RDZADMIN) OMVS(UID(6))
```



O seguinte comando **chown** de amostra do z/OS UNIX altera o proprietário e o grupo de `/var/rdz/pushtoclient` e de tudo que ele contém para RDZADM1 e RDZADMIN, respectivamente. O comando deve ser executado por um superusuário (UID 0) para evitar problemas de permissão.

```
chown -R rdzadm1:rdzadmin /var/rdz/pushtoclient
```

O seguinte comando **chmod** de amostra do z/OS UNIX altera a máscara de bits de permissão de `/var/rdz/pushtoclient` e de tudo que ela contém para 775. Execute-o para assegurar-se de que toda adição manual ao diretório siga a lógica usada pelo Developer for System z. O comando deve ser executado por um superusuário (UID 0) para evitar problemas de permissão.

```
chmod -R 775 /var/rdz/pushtoclient
```

Consulte o *Security Server RACF Command Language Reference* (SA22-7687) para obter mais informações sobre os comandos de amostra do RACF. Consulte o *UNIX System Services Command Reference* (SA22-7802) para obter mais informações sobre os comandos de amostra do z/OS UNIX. Consulte a seção “Estrutura de diretório do z/OS UNIX” na página 15 para obter mais informações.

## Uso de Espaço de Metadados

Os metadados push-to-client usam uma quantidade razoavelmente pequena de espaço em disco no z/OS UNIX, porque a grande massa dos metadados são arquivos XML codificados para UTF-8. Observe que o código do produto usado nos cenários de atualização de cliente podem ser armazenados em qualquer lugar da rede; não é necessário armazenar no z/OS UNIX, porque os metadados push-to-client relacionados (chamados arquivos de resposta) apontam o cliente para o local correto.

---

## Controle de Configuração do Cliente

Quando um cliente do Developer for System z (versão 8.0.1 e superior) se conecta ao host, ele lê as definições em `pushtoclient.properties`. Se a diretiva `config.enabled` estiver ativada, o cliente comparará sua configuração atual com as definições nos metadados push-to-client. Se forem encontradas diferenças, o cliente iniciará um assistente que extrai os dados necessários e ativa a configuração conforme indicado pelo push-to-client.

A diretiva `reject.config.updates` em `pushtoclient.properties` controla se um usuário tem permissão para rejeitar as atualizações de configuração que o push-to-client está prestes a entregar.

Um cliente do Developer for System z (versão 8.0.1 e superior) tem um assistente, a ser usado pelo administrador de cliente, que pode exportar a configuração atual, que por sua vez é importada por todos os clientes do Developer for System z através do push-to-client. Observe que essa função está disponível em todos os clientes; por isso, você deve assegurar que apenas os administradores de cliente tenham permissão de gravação nos diretórios do z/OS UNIX que contêm metadados push-to-client (`/var/rdz/pushtoclient`).

A versão 8.0.3 ou superior é necessária ao cliente e ao host para ativar o suporte de grupo, conforme documentado em “Diversos Grupos de Desenvolvedores” na página 123.

---

## Controle de Versão do Cliente

Quando um cliente do Developer for System z (versão 8.0.1 e superior) se conecta ao host, ele lê as definições em `pushtoclient.properties`. Se a diretiva `product.enabled` estiver ativada, o cliente comparará sua versão de produto atual com as definições nos metadados `push-to-client`. Se forem encontradas diferenças, o cliente iniciará um assistente que extrai os dados necessários e ativa a configuração conforme indicado pelo `push-to-client`.

A diretiva `reject.product.updates` em `pushtoclient.properties` controla se um usuário tem permissão para rejeitar atualizações de produto que o `push-to-client` está prestes a entregar.

A versão 8.0.3 ou superior é necessária ao cliente e ao host para ativar o suporte de grupo, conforme documentado em “Diversos Grupos de Desenvolvedores”.

---

## Diversos Grupos de Desenvolvedores

Desde a versão 8.0.3, o administrador de cliente pode criar diversos conjuntos de configuração de cliente e diversos cenários de atualização de cliente para ajustar as necessidades de diferentes grupos de desenvolvedores. Isso permite que os usuários recebam uma configuração customizada, com base em critérios como associação de um grupo LDAP ou permissão para um perfil de segurança.

### Ativação

O suporte para diversos grupos de desenvolvedores, cada um com seus próprios requisitos de configuração e atualização do cliente, é ativado ao designar o valor desejado às diretivas relacionadas (`config.enabled` e `product.enabled`) em `pushtoclient.properties`, conforme mostrado na Tabela 36.

*Tabela 36. Matriz de suporte ao grupo push-to-client para \*.enabled*

| Valor *.enabled | Função ativada | Diversos grupos suportados                                                                 |
|-----------------|----------------|--------------------------------------------------------------------------------------------|
| False           | Não            | Não                                                                                        |
| True            | Sim            | Não                                                                                        |
| LDAP            | Sim            | Sim, com base na associação de grupos LDAP<br>FEK.PTC. *.ENABLED.sysname.devgroup          |
| SAF             | Sim            | Sim, com base na permissão para perfis de segurança<br>FEK.PTC. *.ENABLED.sysname.devgroup |

Observe que quando a função está ativada (isso inclui o valor TRUE), os desenvolvedores sempre fazem parte de um grupo padrão. Um desenvolvedor pode fazer parte de nenhum, um ou vários grupos adicionais.

A rejeição das atualizações também pode ser feita condicionalmente, conforme mostrado na Tabela 37.

*Tabela 37. Matriz de suporte ao grupo push-to-client para reject. \*.updates*

| Valor reject. *.updates | Função ativada                                                                        |
|-------------------------|---------------------------------------------------------------------------------------|
| False                   | Não                                                                                   |
| True                    | Sim                                                                                   |
| LDAP                    | Depende da associação do grupo LDAP FEK.PTC.REJECT. *.UPDATES.sysname. **             |
| SAF                     | Depende de permissão para o perfil de segurança FEK.PTC.REJECT. *.UPDATES.sysname. ** |

Observe que as diretivas em `pushtoclient.properties` funcionam independentemente umas das outras. Você pode designar qualquer valor suportado a qualquer diretiva. Não há requisito para manter as configurações semelhantes.

Consulte “Seleção de Grupo Baseada em LDAP” na página 127 e “Seleção de Grupo Baseada em SAF” na página 132 para obter detalhes sobre a configuração necessária para a respectiva função. Consulte “(Opcional) `pushtoclient.properties`, Controle de Cliente Baseado em Host” no *Guia de Configuração do Host* (S517-9094) para obter mais informações sobre como ativar o suporte a diversos grupos.

## Concatenações de Grupo

Quando a função `*.enabled` está ativada (isso inclui o valor `TRUE`) em `pushtoclient.properties`, os desenvolvedores sempre fazem parte de um grupo padrão para a função relacionada. Um desenvolvedor pode fazer parte de nenhum, um ou vários grupos adicionais.

Para limitar a complexidade de aplicar mudanças definidas em vários grupos, o Developer for System z limita as definições que serão usadas, como base em uma seleção feita pelo usuário.

*Tabela 38. Concatenações de Grupo Push-to-client*

| Grupos adicionais | Definições usadas            |
|-------------------|------------------------------|
| Nenhum            | Padrão                       |
| Um                | Padrão ou (padrão + grupo)   |
| Diversos          | Padrão ou (padrão + 1 grupo) |

O Developer for System z usa a seguinte lógica ao construir e aplicar o conjunto de mudanças:

1. Aceita as atualizações, se houver, especificadas nas definições padrão.
2. Aceita as atualizações especificadas na definição do grupo selecionado, se houver, alterando aquelas padrão, se já estiverem lá.
3. Aplica as atualizações no cliente.

**Nota:** As atualizações podem consistir em ações de exclusão, inclusão e sobreposição.

## Ligação da Área de Trabalho

Embora um desenvolvedor possa fazer parte de diversos grupos simultaneamente, a área de trabalho ativa do desenvolvedor não pode. A área de trabalho ativa deve ser limitada a um grupo de configuração específico (que pode ser o grupo padrão) e a um grupo de produto específico (que pode ser o grupo padrão) para receber as atualizações da configuração ou do produto. Uma vez feita a ligação, ela não pode ser desfeita. Uma nova área de trabalho deverá ser criada se uma nova ligação de grupo for necessária.

Quando uma área de trabalho que não possui ligações de grupo de configuração se conecta ao host e o `config.enabled` indica que a função distribuir-para-cliente está ativa, o Developer for System z consulta todos os grupos de configuração para determinar a quais grupos o usuário pertence e avisa o usuário para selecionar um grupo. Nas conexões sucessivas, somente o grupo selecionado é consultado para ver se a associação ao grupo ainda é válida.

*Tabela 39. Ligações do grupo de configuração da área de trabalho*

| config.enabled | A área de trabalho limita a esse grupo de atualização de configuração |
|----------------|-----------------------------------------------------------------------|
| False          | Nenhum                                                                |
| True           | Padrão                                                                |
| LDAP           | Padrão ou Grupo (após avisar)                                         |
| SAF            | Padrão ou Grupo (após avisar)                                         |

Quando uma área de trabalho que não possui ligações de grupo de conexão do produto se conecta ao host e o `product.enabled` indica que a função distribuir-para-cliente está ativa, o Developer for System z consulta todos os grupos de produtos para determinar a quais grupos o usuário pertence e avisa o usuário para selecionar um grupo. Nas conexões sucessivas, somente o grupo selecionado é consultado para ver se a associação ao grupo ainda é válida.

*Tabela 40. Ligações do grupo do produto da área de trabalho*

| product.enabled | A área de trabalho limita a esse grupo de atualização do produto |
|-----------------|------------------------------------------------------------------|
| False           | Nenhum                                                           |
| True            | Padrão                                                           |
| LDAP            | Padrão ou Grupo (após avisar)                                    |
| SAF             | Padrão ou Grupo (após avisar)                                    |

As diretivas `reject.*.updates` podem trabalhar com ou sem as definições de grupo. Se os grupos forem utilizados para o `reject.*.updates`, então, a ligação de grupo da diretiva `*.enabled` relacionada é utilizada. Quando uma atualização está presente, o Developer for System z determina se o usuário tem permissão para rejeitar a atualização, e age apropriadamente.

O suporte de grupo para as diretivas `reject.*.updates` é novo na versão 9.1.0 e necessita que tanto o host Developer for System z quando o cliente tenham a versão 9.1.0 ou mais recente. O suporte altera a maneira como as palavras-chave LDAP e SAF são processadas.

Antes da versão 9.1.0, estar na lista de acesso para o `FEK.PTC.REJECT.*.UPDATES.sysname` era suficiente para rejeitar uma atualização, independentemente da ligação de grupo da área de trabalho. Desde a versão 9.1.0, o `FEK.PTC.REJECT.*.UPDATES.sysname` é usado apenas para rejeitar atualizações nas ligações de área de trabalho para o grupo padrão. O limite das áreas de trabalho a um grupo requerem que você esteja na lista de acesso para o `FEK.PTC.REJECT.*.UPDATES.sysname.groupname` para rejeitar as atualizações.

## Local de Metadados do Grupo

Conforme documentado em “Local de Metadados” na página 120, todos os metadados push-to-client são armazenados em uma estrutura de diretório na parte superior de `/var/rdz/pushtoclient/` ao usar uma configuração sem o suporte de grupo. O mesmo layout de dados é mantido quando o suporte de grupo é ativado, mas com uma pequena diferença de interpretação, do diretório base, `/var/rdz/pushtoclient/`:

- Os dados existentes em `/var/rdz/pushtoclient/` são interpretados como os dados do grupo padrão. A exportação para o grupo padrão cria ou atualiza os metadados em `/var/rdz/pushtoclient/`. Essa interpretação assegura a compatibilidade com os clientes versão 8.0.1 e versão 8.0.2, que são ativados para push-to-client, mas não suportam diversos grupos.
- A exportação para um grupo cria ou atualiza os metadados em `/var/rdz/pushtoclient/grouping/<devgroup>/`, como se esse fosse o diretório

base em vez do /var/rdz/pushtoclient/. O valor <devgroup> corresponde ao nome do grupo designado a um grupo específico de desenvolvedores.

A customização do produto inicial cria o diretório grouping/ em /var/rdz/pushtoclient/. O administrador de cliente é responsável por incluir os diretórios <devgroup>/ em /var/rdz/pushtoclient/grouping/.

Observe que durante a customização inicial do produto, os diretórios projects/, install/ e install/responsefiles/ são criados em /var/rdz/pushtoclient/. O administrador do cliente deverá repetir essas ações make-directory em /var/rdz/pushtoclient/grouping/<devgroup>/ se houver necessidade de cenários de upgrade de produto de grupo específico ou projetos baseados em host de grupo específico.

A seguinte sequência de comandos de amostra do z/OS UNIX cria os subdiretórios com a máscara de bits de permissão correta. Os comandos devem ser executados pelo administrador de cliente para evitar problemas de propriedade.

```
saved_umask=$(umask)
umask 0000
cd /var/rdz/pushtoclient/grouping/
mkdir -m775 <devgroup>
cd <devgroup>
mkdir -m775 install
mkdir -m775 install/responsefiles
mkdir -m775 projects
umask $saved_umask
```

Consulte o *UNIX System Services Command Reference* (SA22-7802) para obter mais informações sobre os comandos de amostra do z/OS UNIX.

## Etapas de Configuração

A configuração do suporte para diversos grupos de desenvolvedores requer uma coordenação entre o programador de sistema do z/OS, o administrador de cliente e o administrador que gerencia os critérios de seleção (o administrador de LDAP ou segurança). Na seguinte descrição do fluxo de trabalho, o administrador de segurança gerencia os critérios de seleção:

1. O administrador de cliente solicita ao administrador de segurança as informações sobre configuração de agrupamento existente para desenvolvedores. A reutilização da configuração existente agiliza e simplifica a configuração de push-to-client.
2. O administrador de cliente determina como ele deseja estruturar o suporte de diversos grupos e quem deve fazer parte desses grupos de push-to-client.

### Nota:

- Há sempre uma configuração padrão definida e um cenário de atualização de produto padrão.
  - Os conjuntos de mudanças de push-to-client podem incluir ações de exclusão, inclusão e sobreposição.
  - Os conjuntos de mudanças de push-to-client podem ficar vazios.
  - Um desenvolvedor pode fazer parte de nenhum, um ou vários grupos de push-to-client.
  - O administrador de cliente deve ser membro de cada grupo de push-to-client.
3. Os administradores de cliente e de segurança concordam quanto aos nomes de grupos push-to-client a serem usados.
  4. O administrador de cliente cria o diretório

```
/var/rdz/pushtoclient/grouping/<devgroup>
```

para cada grupo push-to-client.

**Nota:** Os bits de permissão desse diretório devem ser 775 (drwxrwxr-x).

5. O administrador de segurança faz a configuração inicial necessária para definir os perfis dos critérios de seleção push-to-client e inclui os grupos push-to-client nas listas de acesso.

**Nota:**

- As estruturas de critérios de seleção devem ser definidas com pelo menos o administrador de cliente na lista de acesso para que o administrador de cliente possa criar os metadados push-to-client relacionados.
  - Para a configuração inicial, apenas o administrador de cliente deve estar na lista de acesso de um grupo push-to-client. Isso para evitar que os clientes do Developer for System z recebam configurações que estejam em construção.
6. O programador de sistema do z/OS ativa o suporte de diversos grupos ajustando `pushtoclient.properties`.

**Nota:** As diretivas `*.enabled` devem estar ativadas para que o administrador de cliente possa criar os metadados push-to-client relacionados.

7. O administrador de cliente cria as áreas de trabalho de cada grupo e as exporta para o host usando os respectivos nomes dos grupos. O administrador de cliente também cria os arquivos de resposta requeridos para criar cenários de atualização do produto específico do grupo.
8. O administrador de segurança inclui os desenvolvedores nos grupos push-to-client, ativando o push-to-client para os desenvolvedores.

---

## Seleção de Grupo Baseada em LDAP

Embora o protocolo LDAP seja o nome de um protocolo baseado em TCP/IP, ele é comumente usado para descrever um conjunto de serviços de diretório distribuídos. Como um banco de dados, um diretório é uma coleção estruturada de registros. O Developer for System z pode usar um servidor LDAP como um banco de dados hierárquico simples, no qual os grupos contêm um ou mais membros.

Ao usar definições no servidor LDAP como mecanismo de seleção (o valor LDAP é especificado para diretivas em `pushtoclient.properties`), o Developer for System z verifica a associação dos nomes de grupo listados na Tabela 41 para determinar a quais grupos de desenvolvedores o usuário pertence, e se um usuário tem permissão para rejeitar atualizações.

*Tabela 41. Informações do LDAP de Push-to-client*

| Nome do grupo (cn=)                             | Resultado                                                                                                                |
|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| FEK.PTC.CONFIG.ENABLED.sysname.devgroup         | O cliente aceita atualizações de configuração para o grupo especificado                                                  |
| FEK.PTC.PRODUCT.ENABLED.sysname.devgroup        | O cliente aceita atualizações de produto para o grupo especificado                                                       |
| FEK.PTC.REJECT.CONFIG.UPDATES.sysname           | O usuário pode rejeitar as atualizações da configuração quando a área de trabalho estiver limitada ao grupo padrão       |
| FEK.PTC.REJECT.CONFIG.UPDATES.sysname.devgroup  | O usuário pode rejeitar as atualizações da configuração quando a área de trabalho estiver limitada ao grupo especificado |
| FEK.PTC.REJECT.PRODUCT.UPDATES.sysname          | O usuário pode rejeitar as atualizações do produto quando a área de trabalho estiver limitada ao grupo padrão            |
| FEK.PTC.REJECT.PRODUCT.UPDATES.sysname.devgroup | O usuário pode rejeitar as atualizações do produto quando a área de trabalho estiver limitada ao grupo especificado      |

O valor `devgroup` corresponde ao nome do grupo designado a um grupo específico de desenvolvedores. Observe que o nome do grupo é visível nos clientes do Developer for System z.

O valor `sysname` corresponde ao nome do sistema de destino.

Um usuário pode selecionar para ligar uma área de trabalho a um grupo padrão para as atualizações da configuração se o `config.enabled` no `pushtoclient.properties` estiver definido para SAF ou para LDAP. Se o `config.enabled` estiver configurado para `TRUE`, a área de trabalho será automaticamente limitada ao grupo padrão.

Um usuário pode selecionar para ligar uma área de trabalho a um grupo padrão para as atualizações do produto, se o `product.enabled` no `pushtoclient.properties` estiver configurado para SAF ou LDAP. Se o `product.enabled` estiver configurado para `TRUE`, a área de trabalho será automaticamente limitada ao grupo padrão.

Suporte de grupo para as diretivas do `reject.*.updates` é novo na versão 9.1.0 e altera o modo como as palavras-chave LDAP e SAF são processadas.

## Esquema LDAP

O esquema LDAP deve satisfazer às seguintes regras:

1. Cada grupo push-to-client deve ser definido como grupo no esquema.
2. Cada usuário deve ser definido como usuário no esquema.
3. Uma entrada de grupo tem as referências para as entradas do usuário que pertencem a seu próprio grupo.

A Figura 32 é uma definição LDAP de amostra para um grupo e usuário, expressa em formato LDIF.

**Nota:** O Formato de Troca de Dados LDAP (LDIF) é um formato de texto padrão para representar objetos LDAP e atualizações LDAP. Os arquivos que contêm registros LDIF são usados para transferir dados entre servidores de diretório ou como entrada pelos atributos LDAP.

```
Group Definition
dn: cn=FEK.PTC.CONFIG.ENABLED.CDFMVS08.GROUPA,o=PTC,c=DeveloperForZ
objectClass: groupOfUniqueNames
objectClass: top
cn: FEK.PTC.CONFIG.ENABLED.CDFMVS08.GROUPA
description: Project A
uniqueMember: uid=mborn,ou=Users,dc=example,dc=com

User Definition
dn: uid=mborn,ou=Users,dc=example,dc=com
objectClass: organizationalPerson
objectClass: person
objectClass: inetOrgPerson
objectClass: uidObject
objectClass: top
cn: May Born
sn: Born
uid: mborn
facsimiletelephonenumber: +1 800 982 6883
givenname: May
mail: mborn@example.com
ou: Users
```

*Figura 32. Definição de esquema LDAP de amostra*

## Seleção do Servidor LDAP

Há uma ampla seleção de servidores LDAP comerciais e grátis disponíveis. Um exemplo é o IBM Tivoli Directory Server (<http://www-01.ibm.com/software/>)



tivoli/products/directory-server/). Há também um ampla seleção de ferramentas de linha de comandos e baseadas na GUI para gerenciar um servidor LDAP.

Conforme mencionado em “Esquema LDAP” na página 128, cada usuário deve ser definido para o servidor LDAP. Para reduzir o esforço de gerenciamento, é melhor colocar o esquema push-to-client em um servidor LDAP que já tenha acesso a todas as definições de usuário. Por exemplo, você pode usar o IBM Tivoli Directory Server ativo no z/OS usando um banco de dados SDBM (que é um wrapper para seu banco de dados de segurança).

Dependendo das políticas do site, o esquema push-to-client no servidor LDAP pode ser gerenciado pelo administrador de cliente. Esse acordo reduz as necessidades de colaboração, bem como possíveis atrasos e erros de comunicação.

Um argumento em favor do gerenciamento LDAP pelo administrador de cliente é que o esquema push-to-client não contém nada que seja confidencial ou esteja relacionado a segurança. Quando definições de usuário estão disponíveis ao servidor LDAP através de outros esquemas, os objetos LDAP do Developer for System z apenas determinam quais opções um desenvolvedor tem na seleção de um layout de área de trabalho e upgrades automáticos de produtos do cliente do Developer for System z.

## Local do Servidor LDAP

Qualquer servidor de banco de dados que suporte o protocolo LDAP pode ser usado para hospedar o esquema push-to-client do Developer for System z. Portanto, o Developer for System z permite que você especifique as informações necessárias para conectar-se ao servidor LDAP. Também é possível especificar o sufixo que torna o banco de dados exclusivo no servidor LDAP.

| rsed.envvars directive     | Padrão                  |
|----------------------------|-------------------------|
| _RSE_LDAP_SERVER           | Sistema de host local   |
| _RSE_LDAP_PORT             | 389                     |
| _RSE_LDAP_PTC_GROUP_SUFFIX | "O=PTC,C=DeveloperForZ" |

Observe que medidas de segurança de TCP/IP, como firewalls, podem fazer com que o servidor RSE (baseado em host) pare de entrar em contato com o servidor LDAP. Para assegurar-se de que o servidor LDAP possa ser atingido, entre em contato com o administrador de TCP/IP com as seguintes informações:

- Endereço TCP/IP ou nome do DNS do servidor LDAP
- Número da porta do servidor LDAP
- O LDAP usa o protocolo TCP
- O servidor LDAP é contatado pelo servidor RSE baseado em host
- O servidor RSE está ativo em um espaço de endereço RSEDx, em que RSED é o nome da tarefa iniciada do RSE e x é um número aleatório de um dígito

## Configuração de Amostra

Suponha que uma empresa tenha o Developer for System z ativo no sistema CDFMVS08. O IBM Tivoli Directory Server, também ativo no CDFMVS08, é usado como servidor LDAP. O servidor LDAP é configurado conforme descrito em “Incluindo Backend push-to-client no LDAP” na página 130.

Os seguintes usuários utilizam o Developer for System z:

- Desenvolvedores que trabalham em aplicativos financeiros, o ID do usuário BNK010 -> BNK014
- Desenvolvedores que trabalham em aplicativos de seguro, o ID do usuário INS010 -> INS014
- Um administrador de cliente do Developer for System z, ID do usuário RDZADM1

Cada grupo de desenvolvedores requer arquivos de configuração de cliente específicos, e todos os desenvolvedores estão sujeitos ao mesmo controle de versão de cliente. Ao contrário dos administradores de cliente, os desenvolvedores não têm permissão para rejeitar nenhuma mudança que o push-to-client apresente.

Os administradores de cliente e de LDAP concordam em usar os nomes de grupo BANKING e INSURANCE para atualizações de configuração.

## Incluindo Backend push-to-client no LDAP

Neste exemplo, são feitas atualizações no IBM Tivoli Directory Server no z/OS, atualmente usando apenas um banco de dados SDBM (wrapper de banco de dados de segurança), incluindo um banco de dados LDBM (arquivos do z/OS UNIX) para hospedar o esquema push-to-client.

1. Inclua a seção backend do LDBM no arquivo de configuração LDAP.

```
filename ds.conf
restart GLDSRV started task to pick up changes

global section
adminDN "cn=LDAP admin"
adminPW password
listen ldap://:389
schemaPath /etc/ldap

SDBM back-end section (RACF)
database SDBM GLDBSD31/GLDBSD64
suffix "cn=RACF,o=IBM,c=US"

LDBM back-end section (z/OS UNIX files)
database LDBM GLDBLD31/GLDBLD64 LDBM-RDZ
suffix "o=PTC,c=DeveloperForZ"
databaseDirectory /var/ldap/ldbm/rdz
```

2. Pare e inicie a tarefa iniciada do LDAP, GRDSRV, para selecionar as mudanças na configuração.
3. Crie o diretório /var/ldap/ldbm/rdz.

```
mkdir -p /var/ldap/ldbm/rdz
```

4. Atualize o esquema LDAP para incluir o backend do LDBM.

```
ldapmodify -D "cn=LDAP admin" -w password -f
/usr/lpp/ldap/etc/schema.user.ldif

ldapmodify -D "cn=LDAP admin" -w password -f
/usr/lpp/ldap/etc/schema.IBM.ldif
```

5. Inclua a entrada raiz no backend do LDBM.

```
ldapadd -D "cn=LDAP admin" -w password -f
/u/ibmuser/ptc_root.ldif
```

em que /u/ibmuser/ptc\_root.ldif contém o seguinte:

```
dn: o=PTC,c=DeveloperForZ
objectclass: top
objectclass: organization
o: PTC
```

## Configuração de Grupo LDAP Inicial

Inclua os diferentes objetos de grupo LDAP no esquema e torne o administrador de cliente parte de cada um deles. A definição de usuário para o ID do usuário RDZADM1 é extraída do esquema RACF.

```
ldapadd -D "cn=LDAP admin" -w password -f /u/ibmuser/ptc_setup.ldif
```

em que /u/ibmuser/ptc\_setup.ldif contém o seguinte:

```
banking workspace configuration
dn: cn=FEK.PTC.CONFIG.ENABLED.CDFMVS08.BANKING,o=PTC,c=DeveloperForZ
objectclass: groupOfUniqueNames
```

```

cn=FEK.PTC.CONFIG.ENABLED.CDFMVS08.BANKING
description: Developer for System z push-to-client
give client administrator access
uniqueMember: racfID=RDZADM1,profileType=user,cn=RACF,o=IBM,c=US

insurance workspace configuration
dn: cn=FEK.PTC.CONFIG.ENABLED.CDFMVS08.INSURANCE,o=PTC,c=DeveloperForZ
objectclass: groupOfUniqueNames
cn: FEK.PTC.CONFIG.ENABLED.CDFMVS08.INSURANCE
description: Developer for System z push-to-client
give client administrator access
uniqueMember: racfID=RDZADM1,profileType=user,cn=RACF,o=IBM,c=US

reject configuration updates
dn: cn=FEK.PTC.REJECT.CONFIG.UPDATES.CDFMVS08,o=PTC,c=DeveloperForZ
objectclass: groupOfUniqueNames
cn: FEK.PTC.REJECT.CONFIG.UPDATES.CDFMVS08
description: Developer for System z push-to-client
give client administrator access
uniqueMember: racfID=RDZADM1,profileType=user,cn=RACF,o=IBM,c=US

reject product updates
dn: cn=FEK.PTC.REJECT.PRODUCT.UPDATES.CDFMVS08,o=PTC,c=DeveloperForZ
objectclass: groupOfUniqueNames
cn: FEK.PTC.REJECT.PRODUCT.UPDATES.CDFMVS08
description: Developer for System z push-to-client
give client administrator access
uniqueMember: racfID=RDZADM1,profileType=user,cn=RACF,o=IBM,c=US

```

## Incluir Desenvolvedores em Grupos LDAP

Inclua os desenvolvedores nos objetos de grupos LDAP. As definições do usuário para IDs de usuário são obtidas do esquema RACF.

```
ldapmodify -D "cn=LDAP admin" -w password -f /u/ibmuser/ptc_add.ldif
```

em que `/u/ibmuser/ptc_add.ldif` retém o seguinte:

```

banking workspace configuration
dn: cn=FEK.PTC.CONFIG.ENABLED.CDFMVS08.BANKING,o=PTC,c=DeveloperForZ
changeType: modify
add: uniqueMember
uniqueMember: racfID=BNK010,profileType=user,cn=RACF,o=IBM,c=US
uniqueMember: racfID=BNK011,profileType=user,cn=RACF,o=IBM,c=US
uniqueMember: racfID=BNK012,profileType=user,cn=RACF,o=IBM,c=US
uniqueMember: racfID=BNK013,profileType=user,cn=RACF,o=IBM,c=US
uniqueMember: racfID=BNK014,profileType=user,cn=RACF,o=IBM,c=US

insurance workspace configuration
dn: cn=FEK.PTC.CONFIG.ENABLED.CDFMVS08.INSURANCE,o=PTC,c=DeveloperForZ
changeType: modify
add: uniqueMember
uniqueMember: racfID=INS010,profileType=user,cn=RACF,o=IBM,c=US
uniqueMember: racfID=INS011,profileType=user,cn=RACF,o=IBM,c=US
uniqueMember: racfID=INS012,profileType=user,cn=RACF,o=IBM,c=US
uniqueMember: racfID=INS013,profileType=user,cn=RACF,o=IBM,c=US
uniqueMember: racfID=INS014,profileType=user,cn=RACF,o=IBM,c=US

```

## pushtoclient.properties

```

BANKING e INSURANCE têm necessidades de configuração diferentes
config.enabled=LDAP
todos recebem atualizações do produto
product.enabled=TRUE
somente RDZADMIN pode rejeitar atualizações de configuração
reject.config.updates=LDAP
somente RDZADMIN pode rejeitar atualizações de produto
reject.product.updates=LDAP

```

## rased.envvars

Nenhuma atualização é necessária porque os padrões são usados:

- `_RSE_LDAP_SERVER=CDFMVS08.RALEIGH.IBM.COM`
- `_RSE_LDAP_PORT=389`
- `_RSE_LDAP_PTC_GROUP_SUFFIX="o=PTC,c=DeveloperForZ"`

## /var/rdz/pushtoclient/\*install

Ao exportar a configuração da área de trabalho para os grupos BANKING e INSURANCE, o assistente de exportação cria os diretórios `/var/rdz/pushtoclient/grouping/<devgroup>/`, bem como a estrutura de diretório por trás dele.

- `/var/rdz/pushtoclient/grouping/BANKING/*`
- `/var/rdz/pushtoclient/grouping/INSURANCE/*`

Como não há cenários de upgrade de produto individualizado, o administrador de cliente não precisa criar ou atualizar os subdiretórios `install/` e `install/responsefiles/` no `/var/rdz/pushtoclient/grouping/<devgroup>`.

O administrador de cliente deve criar os arquivos de resposta necessários para atualizações do produto no diretório de grupo padrão, /var/rdz/pushtoclient/install/responsefiles/.

## Seleção de Grupo Baseada em SAF

SAF (Security Access Facility) é uma interface para acessar qualquer produto de segurança do z/OS. O Developer for System z pode usar essa interface para consultar o produto de segurança e recuperar informações relacionadas a push-to-client.

Ao usar as definições do banco de dados de segurança como mecanismo de seleção (o valor SAF é especificado para diretivas em `pushtoclient.properties`), o Developer for System z verifica as permissões de acesso aos perfis listados na Tabela 42 para determinar a quais grupos de desenvolvedores o usuário pertence, e se um usuário tem permissão para rejeitar atualizações.

*Tabela 42. Informações do SAF de Push-to-client*

| Perfil FACILITY                                     | Comprimento fixo | Acesso Necessário | Resultado                                                                                                                |
|-----------------------------------------------------|------------------|-------------------|--------------------------------------------------------------------------------------------------------------------------|
| FEK.PTC.CONFIG.ENABLED.<br>sysname.devgroup         | 23               | READ              | O cliente aceita atualizações de configuração para o grupo especificado                                                  |
| FEK.PTC.PRODUCT.ENABLED.<br>sysname.devgroup        | 24               | READ              | O cliente aceita atualizações de produto para o grupo especificado                                                       |
| FEK.PTC.REJECT.CONFIG.<br>UPDATES.sysname           | 30               | READ              | O usuário pode rejeitar as atualizações da configuração quando a área de trabalho estiver limitada ao grupo padrão       |
| FEK.PTC.REJECT.CONFIG. UPDATES.sysname.devgroup     | 30               | READ              | O usuário pode rejeitar as atualizações da configuração quando a área de trabalho estiver limitada ao grupo especificado |
| FEK.PTC.REJECT.PRODUCT.<br>UPDATES.sysname          | 31               | READ              | O usuário pode rejeitar as atualizações do produto quando a área de trabalho estiver limitada ao grupo padrão            |
| FEK.PTC.REJECT.PRODUCT.<br>UPDATES.sysname.devgroup | 31               | READ              | O usuário pode rejeitar as atualizações do produto quando a área de trabalho estiver limitada ao grupo especificado      |

**Nota:** O Developer for System z presume que um usuário não tenha autorização de acesso quando o software de segurança indica que ele não pode determinar se um usuário tem ou não autorização de acesso a um perfil. Um exemplo disso é quando o perfil não está definido.

O valor `devgroup` corresponde ao nome do grupo designado a um grupo específico de desenvolvedores. Observe que o nome do grupo é visível nos clientes do Developer for System z.

O valor `sysname` corresponde ao nome do sistema de destino.

Um usuário pode selecionar para ligar uma área de trabalho a um grupo padrão para as atualizações da configuração se o `config.enabled` no `pushtoclient.properties` estiver configurado para SAF ou LDAP. Se o

config.enabled estiver configurado para TRUE, a área de trabalho será automaticamente limitada ao grupo padrão.

Um usuário pode selecionar para ligar uma área de trabalho a um grupo padrão para as atualizações do produto se o product.enabled no pushtoclient.properties estiver configurado para SAF ou LDAP. Se o product.enabled estiver configurado para TRUE, a área de trabalho será automaticamente limitada ao grupo padrão.

A coluna “Comprimento fixo” documenta o comprimento da parte fixa do perfil de segurança relacionado.

Por padrão, o Desenvolvedor para System z espera que os perfis FEK.\* estejam na classe de segurança FACILITY. Observe que os perfis na classe FACILITY estão limitados a 39 caracteres. Se a soma do comprimento da parte de perfil fixo (FEK.PTC.<key>.) e o comprimento da parte de perfil específico do site (sysname ou sysname.devgroup) exceder esse número, você poderá colocar os perfis em outra classe e instruir o Developer for System z a usar essa classe no lugar. Para fazer isso, remova o comentário da linha \_RSE\_FEK\_SAF\_CLASS em rsed.envvars e forneça o nome de classe desejado.

## Configuração de Amostra

Suponha que uma empresa tenha o Developer for System z ativo no sistema CDFMVS08. O banco de dados de segurança RACF é compartilhado entre diversos sistemas e os grupos a seguir são definidos no banco de dados de segurança:

- DEVBANK: desenvolvedores que trabalham em aplicativos financeiros
- DEVINSUR: desenvolvedores que trabalham em aplicativos de seguro
- RDZADMIN: administradores de cliente do Developer for System z

Cada grupo de desenvolvedores requer arquivos de configuração de cliente específicos, e todos os desenvolvedores estão sujeitos ao mesmo controle de versão de cliente. Ao contrário dos administradores de cliente, os desenvolvedores não têm permissão para rejeitar nenhuma mudança que o push-to-client apresente. A regra de rejeição é válida para todos os sistemas, em preparação para expansão futura.

Os administradores de cliente e de segurança concordam em usar os nomes de grupo de push-to-client, BANKING e INSURANCE, para atualizações de configuração.

## Definição de Segurança

Os perfis são definidos na classe XFACILIT devido ao nome do perfil mais longo, o FEK.PTC.REJECT.PRODUCT.UPDATE.CDFMVS08.DEVINSUR possui 48 caracteres de comprimento, que é acima dos 39 caracteres suportados pela classe FACILITY.

```
permitir que RDZADMIN e DEVBANK selecionem o grupo de push-to-client BANKING
RDEFINE XFACILIT (FEK.PTC.CONFIG.ENABLED.CDFMVS08.BANKING) -
 UACC(NONE) DATA('RATIONAL DEVELOPER FOR SYSTEM Z - PUSH-TO-CLIENT')
PERMIT FEK.PTC.CONFIG.ENABLED.CDFMVS08.BANKING CLASS(XFACILIT) -
 ID(RDZADMIN DEVBANK) ACCESS(READ)

permitir que RDZADMIN e DEVINSUR seleccione o grupo de push-to-client INSURANCE
RDEFINE XFACILIT (FEK.PTC.CONFIG.ENABLED.CDFMVS08.INSURANCE) -
 UACC(NONE) DATA('RATIONAL DEVELOPER FOR SYSTEM Z - PUSH-TO-CLIENT')
PERMIT FEK.PTC.CONFIG.ENABLED.CDFMVS08.INSURANCE CLASS(XFACILIT) -
 ID(RDZADMIN DEVINSUR) ACCESS(READ)

RDZADMIN pode rejeitar as atualizações da configuração em qualquer
sistema e para qualquer grupo
RDEFINE XFACILIT (FEK.PTC.REJECT.CONFIG.UPDATE.***) -
 UACC(NONE) DATA('RATIONAL DEVELOPER FOR SYSTEM Z - PUSH-TO-CLIENT')
PERMIT FEK.PTC.REJECT.CONFIG.UPDATE.** CLASS(XFACILIT) -
 ID(RDZADMIN) ACCESS(READ)

RDZADMIN pode rejeitar as atualizações do produto em qualquer
sistema e para qualquer grupo
RDEFINE XFACILIT (FEK.PTC.REJECT.PRODUCT.UPDATE.***) -
```

```
UACC(NONE) DATA('RATIONAL DEVELOPER FOR SYSTEM Z - PUSH-TO-CLIENT')
PERMIT FEK.PTC.REJECT.PRODUCT.UPDATES.** CLASS(XFACILIT) -
 ID(RDZADMIN) ACCESS(READ)

ativar mudanças
SETROPTS RACLIST(XFACILIT) REFRESH
```

## pushtoclient.properties

```
BANKING e INSURANCE têm necessidades de configuração diferentes
config.enabled=SAF
todos recebem atualizações do produto
product.enabled=TRUE
somente RDZADMIN pode rejeitar atualizações de configuração
reject.config.updates=SAF
somente RDZADMIN pode rejeitar atualizações de produto
reject.product.updates=SAF
```

## rsed.envvars

```
_RSE_FEK_SAF_CLASS=XFACILIT
```

## /var/rdz/pushtoclient/\*install

Ao exportar a configuração da área de trabalho para os grupos BANKING e INSURANCE, o assistente de exportação cria os diretórios /var/rdz/pushtoclient/grouping/<devgroup>/, bem como a estrutura de diretório por trás dele.

- /var/rdz/pushtoclient/grouping/BANKING/\*
- /var/rdz/pushtoclient/grouping/INSURANCE/\*

Como não há cenários de upgrade de produto individualizado, o administrador de cliente não precisa criar ou atualizar os subdiretórios install/ e install/responsefiles/ no /var/rdz/pushtoclient/grouping/<devgroup>/.

O administrador de cliente deve criar os arquivos de resposta necessários para atualizações do produto no diretório de grupo padrão, /var/rdz/pushtoclient/install/responsefiles/.

## Período de Carência para Rejeitar Mudanças

Suponha que enquanto a configuração de amostra está ativa, um fix pack do Developer for System z com correções importantes se torne disponível, mas o cronograma de um projeto financeiro faz com que vários desenvolvedores estejam muito ocupados para alterar qualquer coisa em suas estações de trabalho imediatamente.

Para resolver o problema, o administrador de segurança pode conceder a todos os desenvolvedores DEVBANK um período de carência durante o qual eles podem optar por adiar (rejeitar) a atualização.

Configurar o período de carência é um processo muito simples:

```
start of grace period
PERMIT FEK.PTC.REJECT.PRODUCT.UPDATES.** CLASS(XFACILIT) -
 ID(DEVBANK) ACCESS(READ)

ativar mudanças
SETROPTS RACLIST(FACILITY) REFRESH
```

Ao final do período de carência, a autoridade adicional pode ser removida novamente:

```
end of grace period
PERMIT FEK.PTC.REJECT.PRODUCT.UPDATES.** CLASS(XFACILIT) -
 ID(DEVBANK) DELETE

ativar mudanças
SETROPTS RACLIST(FACILITY) REFRESH
```

**Nota:** O administrador de segurança também poderia ter criado um perfil de FEK.PTC.REJECT.PRODUCT.UPDATES.\*.DEVBANK com UACC(READ). Isso permitiria a todos os desenvolvedores, que limitam suas áreas de trabalho, acessassem o grupo DEVBANK para rejeitar as atualizações do produto. A permissão de rejeição não é

concedida a desenvolvedores que limitam suas áreas de trabalho ao grupo padrão, mesmo que sejam membros do grupo DEVBANK, já que isso é controlado pelo perfil do FEK.PTC.REJECT.PRODUCT.UPDATES.\*.

---

## Projetos baseados no host

Os projetos do z/OS podem ser definidos individualmente por meio da perspectiva Projetos do z/OS no cliente, ou podem ser definidos centralmente no host e propagados para o cliente em uma base por usuário individual. Esses "projetos baseados em host" se parecem e funcionam exatamente como os projetos definidos no cliente, exceto que sua estrutura, seus membros e suas propriedades não podem ser modificados pelo cliente e só podem ser acessados quando conectados ao host.

O diretório base para projetos baseados em host é definido (pelo administrador do cliente) em `/var/rdz/pushtoclient/keymapping.xml`, e é `/var/rdz/pushtoclient/projects` por padrão.

Para configurar projetos baseados em host, o gerente de projeto ou o desenvolvedor líder precisa definir os seguintes tipos de arquivos de configuração. Todos os arquivos são XML codificados para UTF-8.

- Os arquivos de instância de projeto são específicos de um único ID do usuário e apontam para arquivos de definição de projeto reutilizáveis. Cada usuário que trabalha com projetos baseados em host precisa de um subdiretório, `/var/rdz/pushtoclient/projects/<userid>/`, contendo um arquivo de instância de projeto (`*.hbpin`) para cada projeto a ser transferido por download.
- Os arquivos de definição de projeto definem a estrutura e o conteúdo do projeto e podem ser reutilizados por diversos usuários. Os arquivos de definição de projeto (`*.hbppd`) listam os subprojetos contidos pelo projeto e estão localizados no diretório de definição de projeto raiz ou em um de seus subdiretórios.
- Os arquivos de definição de subprojeto definem a estrutura e o conteúdo do subprojeto e podem ser reutilizados por diversos usuários. Os arquivos de definição de subprojeto (`*.hbpsd`) definem o conjunto de recursos requeridos para construir um único módulo de carregamento e estão localizados no diretório definição de projeto raiz ou em um de seus subdiretórios.
- Os arquivos de propriedades de subprojeto são arquivos de propriedades com suporte a substituição de variável e podem ser reutilizados por diversos subprojetos. Os arquivos de propriedade de subprojeto (`*.hbppr`) suportam substituição de variável para permitir compartilhamento de arquivos de propriedade entre diversos usuários e estão localizados no diretório de definição de projeto raiz ou em um de seus subdiretórios.

Os projetos baseados em host também são elegíveis para participar da configuração de diversos grupos discutida em “Diversos Grupos de Desenvolvedores” na página 123. Essa elegibilidade significa que os projetos baseados em host podem ser definidos também em `/var/rdz/pushtoclient/grouping/<devgroup>/projects/`.

Quando uma área de trabalho está ligada a um grupo específico, e há definições de projeto para um usuário nesse grupo e no grupo padrão, o usuário recebe as definições do projeto dos grupos padrão e específico.





---

## Capítulo 8. considerações CICSTS

Tradicionalmente, a função de definição de recursos para o CICS tem sido o domínio do administrador do CICS. Há uma resistência em permitir que o desenvolvedor de aplicativos defina recursos do CICS por vários motivos:

- A maioria das definições de recursos do CICS tem muitos parâmetros que, devido à complexidade, ao inter-relacionamento com outras definições de recurso e aos padrões de compra, requerem conhecimento de administrador do CICS para obter uma definição correta. Definições incorretas podem causar resultados inesperados que podem afetar a região inteira do CICS.
- A maioria das lojas de clientes fornece ambientes de desenvolvimento e de teste do CICS que devem estar disponíveis para uso compartilhado por vários grupos de aplicativos e desenvolvedores. Muitas lojas de cliente têm Acordos de Nível de Serviço em vigor para esses ambientes. Para atender a esses contratos, é necessário controle estrito dos ambientes.

Developer for System z aborda esses problemas permitindo que os administradores do CICS controlem padrões de definição de recurso do CICS e controlem as propriedades de exibição de um parâmetro de definição de recurso do CICS por meio do servidor CICS Resource Definition (CRD), que é parte do Application Deployment Manager.

Por exemplo, o administrador do CICS pode fornecer certos parâmetros de definição de recurso do CICS que podem não ser atualizados pelo desenvolvedor de aplicativos. Outros parâmetros de definição de recurso do CICS podem ser atualizados, com ou sem os padrões fornecidos, ou o parâmetro de definição de recurso do CICS pode ser ocultado para evitar uma complexidade desnecessária.

Quando o desenvolvedor de aplicativos estiver satisfeito com as definições de recursos do CICS, elas poderão ser instaladas imediatamente no ambiente de teste do CICS em execução, ou poderão ser exportadas em um manifesto para edição e aprovação adicionais por um administrador do CICS. O administrador do CICS pode utilizar o administrative utility (utilitário em lote) ou a ferramenta Processamento de Manifesto para implementar as alterações de definição de recurso.

**Nota:** A ferramenta Processamento de Manifesto é um plug-in para o IBM CICS Explorer.

Consulte "(Opcional) Gerenciador de Implementação do Aplicativo" no *Guia de Configuração do Host* (SC23-7658) para obter mais informações sobre as tarefas necessárias para configurar o Application Deployment Manager em seu sistema host.

Customizar o Application Deployment Manager inclui os serviços a seguir no Developer for System z:

- (no cliente) O IBM CICS Explorer fornece uma infraestrutura baseada em Eclipse para visualizar e gerenciar recursos CICS e possibilita maior integração entre as ferramentas CICS
- (no cliente) O editor CICS Resource Definition (CRD)
- (no host) O servidor CICS Resource Definition (CRD), que é executado como um aplicativo CICS

O servidor CICS Resource Definition (CRD) do Application Deployment Manager consiste no próprio servidor CRD, um repositório CRD, definições do recurso CICS associadas e, ao usar a interface de Serviço da Web, arquivos de ligação de Serviço da Web e um manipulador de mensagens do pipeline de amostra. O servidor CRD deve executar em uma Web Owning Region (WOR), que é mencionada na documentação do Developer for System z como a região de conexão primária do CICS.

Consulte o Centro de Informações do Developer for System z ([http://www-01.ibm.com/support/knowledgecenter/SSQ2R2\\_9.1.0/com.ibm.etools.getstart.wsentdev.doc/kc\\_version\\_welcome\\_rdz.html](http://www-01.ibm.com/support/knowledgecenter/SSQ2R2_9.1.0/com.ibm.etools.getstart.wsentdev.doc/kc_version_welcome_rdz.html)) para saber mais sobre os serviços do Gerenciamento de Implementação de Aplicativo disponível na atual liberação do Developer for System z.

---

## RESTful versus Serviços da Web

O CICS Transaction Server fornece na versão 4.1 e posterior suporte para uma interface HTTP projetada usando princípios do Representational State Transfer (RESTful). Essa interface RESTful é agora a interface CICSTS estratégica para uso por aplicativos clientes. A interface de Serviço da Web mais antiga foi estabilizada e os aprimoramentos serão apenas para a interface RESTful.

O Application Deployment Manager segue essa instrução de direção e exige o servidor RESTful CRD para todos os serviços que são novos no Developer for System versão 7.6 ou superior.

O RESTful e as interfaces de Serviço da Web podem ser ativados simultaneamente em uma única região CICS, se desejado. Nesse caso, haverá dois servidores CRD ativos na região. Os dois servidores compartilharão o mesmo repositório CRD. Observe que o CICS emitirá alguns avisos sobre definições duplicadas quando a segunda interface for definida para a região.

---

## Regiões de Conexão Primária versus não primária

Um ambiente de teste do CICS pode consistir de várias regiões Multi-Region Option (MRO) conectadas. Com o tempo, foram utilizadas designações não oficiais para classificar essas regiões. As designações típicas são Terminal Owning Region (TOR), Web Owning Region (WOR), Application Owning Region (AOR) e Data Owning Region (DOR).

Uma Web Owning Region é usada para implementar suporte aos Serviços da Web do CICS e o servidor CICS Resource Definition (CRD) do Application Deployment Manager deve ser executado nessa região. Esta região é conhecida no Gerenciador de Implementação do Aplicativo como a região de conexão primária do CICS. O cliente do CRD implementa uma conexão de serviço da Web na região de conexão primária do CICS.

As regiões de conexão não primárias do CICS são todas as outras regiões que o servidor CRD pode atender. Esse serviço inclui visualizar recursos utilizando IBM CICS Explorer e definir recursos utilizando o editor de definição de recurso do CICS.

Se o CICSplex SM Business Application Services (BAS) for usado para gerenciar as definições de recurso do CICS da região de conexão primária do CICS, todas as outras regiões do CICS gerenciadas pelo BAS poderão ser atendidas pelo servidor CRD.

As regiões do CICS não gerenciadas pelo BAS requerem alterações adicionais para poderem ser atendidas pelo servidor CRD.

---

## Log de Instalação de Recurso do CICS

As ações feitas pelo servidor CRD em relação aos recursos do CICS são registradas na fila do CICS CSDL TD, que normalmente aponta para a DD MSGUSR de sua região do CICS.

Se o CICSplex SM Business Application Services (BAS) for usado para gerenciar as definições de recursos do CICS, a diretiva CICSplex SM EYUPARM BASLOGMSG deverá ser configurada como (YES) para que o log seja criado.

---

## segurança do Application Deployment Manager

### segurança do repositório CRD

O conjunto de dados de VSAM do repositório do servidor CRD contém todas as definições de recurso padrão e deve, portanto, ser protegido contra atualizações, mas os desenvolvedores devem ter permissão para ler os valores armazenados aqui. Consulte “Definir Perfis de Conjuntos de Dados” na página 54 para obter comandos RACF de amostra para proteger o repositório do CRD.

### Segurança de Pipeline

Quando uma mensagem SOAP for recebida pelo CICS por meio da interface de Serviço da Web, ela será processada por um pipeline. Um pipeline é um conjunto de manipuladores de mensagens que são executados em sequência. O CICS lê o arquivo de configuração do pipeline para determinar quais manipuladores de mensagens devem ser chamados no pipeline. Um manipulador de mensagem é um programa no qual você pode executar processamento especial de pedidos e respostas de serviço da Web.

O Application Deployment Manager fornece um arquivo de configuração de pipeline de amostra que especifica a chamada de um manipulador de mensagens e um programa de processamento de cabeçalho SOAP.

O manipulador de mensagens do pipeline (ADNTMSGH) é usado para segurança através do processamento do ID do usuário e da senha no cabeçalho SOAP. ADNTMSGH é referido pelo arquivo de configuração de pipeline de amostra e, portanto, deve ser colocado na concatenação RPL do CICS.

### Segurança da Transação

CPIH é o ID da transação padrão que um aplicativo chamado por um pipeline executará. Geralmente, o CPIH é configurado para um nível mínimo de autorização.

O Developer for System z fornece várias transações que são usadas pelo servidor CRD durante a definição e a consulta de recursos do CICS. Esses IDs de transação são configurados pelo servidor CRD, dependendo da operação solicitada. Consulte “(Opcional) Gerenciador de Implementação do Aplicativo” no *Guia de Configuração do Host* (SC23-7658) para obter mais informações sobre como customizar os IDs de transação.

| Transação | Descrição                                                                                                                                                                                               |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ADMS      | Para solicitações da ferramenta Processamento de Manifesto para alterar recursos do CICS. Geralmente, isso é destinado aos administradores do CICS. Essa transação requer um alto nível de autorização. |
| ADMI      | Para pedidos que definam, instalem ou desinstalem recursos do CICS. Essa transação pode requerer um nível médio de autorização, dependendo das políticas do site.                                       |
| ADMR      | Para todos os outros pedidos que recuperam as informações de ambiente e de recurso do CICS. Essa transação pode requerer um nível mínimo de autorização, dependendo das políticas do site.              |

Alguns ou todos esses pedidos de definição de recurso feitos pelas transações do servidor CRD devem ser protegidos. No mínimo, os comandos de atualização (parâmetros de atualização padrão do serviço da Web, parâmetros padrão do descritor e o nome de arquivo para ligação do nome do conjunto de dados) devem ser protegidos para impedir que todos, exceto os administradores do CICS, emitam esses comandos usados para configurar padrões de recurso global.

Quando a transação é conectada, a verificação de segurança de recurso do CICS, se ativada, garante que o ID do usuário esteja autorizado para executar o ID de transação.

A verificação de recursos é controlada pela opção RESSEC na transação que está executando o parâmetro de inicialização do sistema RESSEC e, para o servidor do CRD, o parâmetro de inicialização do sistema XPCT.

A verificação de recursos ocorre apenas se o parâmetro de inicialização do sistema XPCT tiver um valor diferente de N0 e a opção RESSEC da definição TRANSACTION for YES ou o parâmetro de inicialização do sistema RESSEC for ALWAYS.

Os seguintes comandos RACF mostram como as transações do servidor CRD podem ser protegidas. Consulte o *RACF Security Guide for CICSTS* para obter informações adicionais sobre a definição da segurança do CICS.

- RALTER GCICSTRN SYSADM UACC(NONE) ADDMEM(ADMS)
- PERMIT SYSADM CLASS(GCICSTRN) ID(#cicsadmin)
- RALTER GCICSTRN DEVELOPER UACC(NONE) ADDMEM(ADMI)
- PERMIT DEVELOPER CLASS(GCICSTRN) ID(#cicsdeveloper)
- RALTER GCICSTRN ALLUSER UACC(READ) ADDMEM(ADMR)
- SETROPTS RACLIST(TCICSTRN) REFRESH

## comunicação criptografada por SSL

A criptografia SSL do fluxo de dados é suportada quando o cliente do Application Deployment Manager usa a interface dos Serviços da Web para invocar o servidor CRD. O uso de SSL para essa comunicação é controlado pela palavra-chave SSL(YES) na definição CICSTS TCIPSERVICE, conforme documentado em *RACF Security Guide para CICSTS*.

## Segurança do Recurso

O CICSTS fornece a capacidade de proteger os recursos e os comandos para manipulá-los. Algumas ações do Application Deployment Manager podem falhar se a segurança estiver ativada, mas não configurada completamente (por exemplo, concedendo permissões para manipular novos tipos de recursos).

Em caso de falha da função no Application Deployment Manager, examine o log do CICS para obter mensagens como a seguir e execute as ações corretivas, conforme documentado em *RACF Security Guide para CICSTS*.

```
DFHXS1111 %date %time %applid %trandid Security violation by user
%userid at netname %portname for resource %resource in class
%classname. SAF codes are (X'safresp',X'safreas'). ESM codes are
(X'esmresp',X'esmreas').
```

---

## Administrative Utility

O Developer for System z fornece o utilitário administrativo para permitir que administradores do CICS forneçam os valores-padrão para as definições de recurso do CICS. Esses padrões podem ser somente de leitura ou podem ser editados pelo desenvolvedor de aplicativos.

O administrative utility fornece as seguintes funções:

- Nome do CICSplex para ambientes de teste gerenciados pelo CICSplex
- Nome do grupo de migração de dados do CICSplex SM
- Configuração da regra de exportação do manifesto
- Padrões de atributo de recurso do CICS e permissões de exibição
- Ligação lógica para física do CICS usada para definições de conjuntos de dados VSAM

O administrative utility é chamado pela tarefa de amostra ADNJSPAU no conjunto de dados FEK.#CUST.JCL. O uso desse utilitário requer acesso UPDATE ao repositório do CRD.

ADNJSPAU está localizado em FEK.#CUST.JCL, a menos que o programador do sistema z/OS tenha especificado um local diferente quando customizou e enviou a tarefa FEK.SFEKSAMP(FEKSETUP). Consulte "Configuração de customização" no *Guia de Configuração do Host* (SC23-7658) para obter mais detalhes.

**Nota:** O repositório CRD deve ser fechado no CICS antes de executar a tarefa ADNJSPAU. O repositório pode ser aberto novamente após a conclusão da tarefa. Por exemplo, após se conectar ao CICS, digite os seguintes comandos para fechar e abrir o arquivo, respectivamente:

- CEMT S FILE(ADNREPF0) CLOSED
- CEMT S FILE(ADNREPF0) OPEN

As instruções de controle de entrada são usadas para atualizar o repositório do CRD de um ambiente de teste do CICS, para o qual as regras gerais de sintaxe a seguir se aplicam:

- Um asterisco na posição 1 indica uma linha de comentário.
- Um comando DEFINE deve iniciar na posição 1, seguido por um único espaço e seguido por uma palavra-chave válida, como TRANSACTION.
- Um valor de palavra-chave deve existir imediatamente após uma palavra-chave. Não são permitidos espaços entre eles. A única exceção é para a exibição das palavras-chave de permissão UPDATE, PROTECT e HIDDEN, que não têm valores.

- Os valores de palavra-chave são colocados entre parênteses.
- Uma palavra-chave e seu valor devem estar contidos em uma única linha.

As definições de amostra a seguir seguem a estrutura dos comandos DFHCSDUP, conforme definido no *CICS Resource Definition Guide para CICSTS*. A única diferença é a inserção das seguintes palavras-chave de permissão de exibição usadas para agrupar valores de atributo em três conjuntos de permissões:

|         |                                                                                                                                                                                     |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UPDATE  | Os atributos que seguem essa palavra-chave serão atualizados por um desenvolvedor de aplicativos utilizando Developer for System z. Esse também é o padrão para atributos omitidos. |
| PROTECT | Os atributos que seguem essa palavra-chave serão exibidos, mas estarão protegidos contra atualizações por um desenvolvedor de aplicativos utilizando Developer for System z.        |
| HIDDEN  | Os atributos que seguem essa palavra-chave não serão exibidos e estarão protegidos contra atualizações por um desenvolvedor de aplicativos utilizando Developer for System z.       |

Consulte a seguinte amostra de código ADNJSPAU.

```
//ADNJSPAU JOB <JOB PARAMETERS>
/*
//ADNJSPAU EXEC PGM=ADNJSPAU,REGION=1M
//STEPLIB DD DISP=SHR,DSN=FEC.SFEKLOAD
//ADMREP DD DISP=OLD,DSN=FEC.#CUST.ADNREPFO
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
*
* Parâmetros CICSplex SM
*
*
* DEFINE CPSMNAME()
*DEFINE STAGINGGROUPNAME(ADMSTAGE)
*
* Regra de exportação de manifesto
*
*DEFINE MANIFESTEXPORTRULE(installOnly)
*
* Padrões de definição de recurso do CICS
* Atributos omitidos são padronizados como UPDATE.
*
* Atributos padrão DB2TRAN
*
*DEFINE DB2TRAN()
* UPDATE DESCRIPTION()
* ENTRY()
* TRANSID()
*
* Atributos padrão DOCTEMPLATE
*
*DEFINE DOCTEMPLATE()
* UPDATE DESCRIPTION()
* TEMPLATENAME()
* FILE() TSQUEUE() TDQUEUE() PROGRAM() EXITPGM()
* DDNAME(DFHHTML) MEMBERNAME()
* HFSFILE()
* APPENDCRLF(YES) TYPE(EBCDIC)
*
* Atributos padrão de arquivo
*
*DEFINE FILE()
* UPDATE DESCRIPTION()
* RECORDSIZE() KEYLENGTH()
* RECORDFORMAT(V) ADD(NO)
* BROWSE(NO) DELETE(NO) READ(YES) UPDATE(NO)
* REMOTESYSTEM() REMOTENAME()
* PROTECT DSNAME() RLSACCESS(NO) LSRPOOLID(1) STRINGS(1)
* STATUS(ENABLED) OPENTIME(FIRSTREF)
* DISPOSITION(SHARE) DATABUFFERS(2) INDEXBUFFERS(1)
* TABLE(NO) MAXNUMRECS(NOLIMIT)
* READINTEG(UNCOMMITTED) DSNSHARING(ALLREQS)
* UPDITEMODEL(LOCKING) LOAD(NO)
* JNLREAD(NONE) JOURNAL(NO)
* JNLSCREAR(NO) JNLUPDATE(NO)
* JNLADD(NONE) JNLSCWRITE(YES)
* RECOVERY(NONE) FWDRECOVLOG(NO)
* BACKUPTYPE(STATIC)
* PASSWORD() NSRGROUP()
* CFDTPOOL() TABLNAME()
```

Figura 33. ADNJSPAU - Administrative utility do CICSTS



```

*
* Atributos padrão Mapset
*
DEFINE MAPSET()
 UPDATE DESCRIPTION()
 PROTECT RESIDENT(NO) STATUS(ENABLED)
 USAGE(NORMAL) USELPACOPY(NO)
** Atributos padrão de tipo de processo
*
DEFINE PROCESSTYPE()
 UPDATE DESCRIPTION()
 FILE(BTS)
 PROTECT STATUS(ENABLED)
 AUDITLOG() AUDITLEVEL(OFF)

*
* Atributos padrão de programa
*
DEFINE PROGRAM()
 UPDATE DESCRIPTION()
 CEDF(YES) LANGUAGE(LE370)
 REMOTESYSTEM() REMOTENAME() TRANSID()
 PROTECT API(CICSAPI) CONCURRENCY(QUASIRENT)
 DATALOCATION(ANY) DYNAMIC(NO)
 EXECKEY(USER) EXECUTIONSET(FULLAPI)
 RELOAD(NO) RESIDENT(NO)
 STATUS(ENABLED) USAGE(NORMAL) USELPACOPY(NO)
 HIDDEN JVM(NO) JVMCLASS() JVMPROFILE(DFHJVMPR)

*
* Atributos padrão TDQueue
*
DEFINE TDQUEUE()
 UPDATE DESCRIPTION()
 TYPE(INTRA)

* Parâmetros de partição extra
 DDNAME() DSNNAME()
 REMOTENAME() REMOTESYSTEM() REMOTELLENGTH(1)
 RECORDSIZE() BLOCKSIZE(0) RECORDFORMAT(UNDEFINED)
 BLOCKFORMAT() PRINTCONTROL() DISPOSITION(SHR)

* Parâmetros de partição intra
 FACILITYID() TRANSID() TRIGERRLEVEL(1)
 USERID()

* Parâmetros indiretos
 INDIRECTNAME()
 PROTECT WAIT(YES) WAITACTION(REJECT)

* Parâmetros de partição extra
 DATABUFFERS(1)
 SYSOUTCLASS() ERROROPTION(IGNORE)
 OPENTIME(INITIAL) REWIND(LEAVE) TYPEFILE(INPUT)

* Parâmetros de partição intra
 ATIFACILITY(TERMINAL) RECOVSTATUS(NO)

```

*Figura 34. ADNJSPAU - Utilitário Administrativo CICSTS (Parte 2 de 3)*

```

*
* Atributos padrão de transação
*
DEFINE TRANSACTION()
 UPDATE DESCRIPTION()
 PROGRAM()
 TWASIZE(0)
 REMOTESYSTEM() REMOTENAME() LOCALQ(NO)
 PROTECT PARTITIONSET() PROFILE(DFHICST)
 DYNAMIC(NO) ROUTABLE(NO)
 ISOLATE(YES) STATUS(ENABLED)
 RUNAWAY(SYSTEM) STORAGECLEAR(NO)
 SHUTDOWN(DISABLED)
 TASKDATAKEY(USER) TASKDATALOC(ANY)
 BREXIT() PRIORITY(1) TRANCLASS(DFHTCL00)
 DTIMOUT(NO) RESTART(NO) SPURGE(NO) TPURGE(NO)
 DUMP(YES) TRACE(YES) CONFDATA(NO)
 OTSTIMEOUT(NO) WAIT(YES) WAITTIME(00,00,00)
 ACTION(BACKOUT) INDOUBT(BACKOUT)
 RESSEC(NO) CMDSEC(NO)
 TRPROF()
 ALIAS() TASKREQ()
 XTRANID() TPNAME() XTPNAME()

*
* Atributos URIMAP
*
DEFINE URIMAP()
 UPDATE USAGE(CLIENT)
 DESCRIPTION()
 PATH(/required/path)
 TCPIPSERVICE()
 TRANSACTION()
 PROGRAM()
 PROTECT ANALYZER(NOANALYZER)
 ATOMSERVICE()
 CERTIFICATE()
 CHARACTERSET()
 CIPHERS()
 CONVERTER()
 HFSFILE()
 HOST(host.mycompany.com)
 HOSTCODEPAGE()
 LOCATION()
 MEDIATYPE()
 PIPELINE()
 PORT(NO)
 REDIRECTTYPE(NONE)
 SCHEME(HTTP)
 STATUS(ENABLED)
 TEMPLATENAME()
 USERID()
 WEBSERVICE()

*
* Nome de arquivo opcional para ligações de nome do conjunto de dados VSAM
*
*DEFINE DSBINDING() DSNNAME()
/*

```

Figura 35. ADNJSAPU - Utilitário Administrativo CICSTS (Parte 3 de 3)

## Notas de Migração do Utilitário Administrativo

Developer for System z versão 7.6.1 incluiu suporte URIMAP no Administrative utility. Para poder usar o suporte URIMAP, o conjunto de dados VSAM do repositório CRD deve estar alocado com um tamanho de registro máximo de 3000. Até a Developer for System z versão 7.6.1, as tarefas de alocação do repositório CRD da amostra usam um tamanho de registro máximo de 2000.

Siga estas etapas para ativar o suporte URIMAP se você estiver ' usando um repositório CRD mais antigo:

1. Crie um backup do seu repositório CRD existente, FEK.#CUST.ADNREPF0.
2. Exclua o repositório CRD existente.
3. Customize e submeta a tarefa FEK.SFEKSAMP(ADNVCRD) para alocar e inicializar um novo repositório CRD. Consulte a documentação no membro para obter instruções de customização.
4. Customize e submeta a tarefa FEK.SFEKSAMP(ADNJSAPU) para usar o Administrative utility para preencher o repositório CRD novo.

**Nota:**

- Migrar o repositório CRD existente não é necessário porque o administrative utility substitui os conteúdos completos do repositório CRD cada vez que ele é executado.
- Não há problemas de compatibilidade de versão com o repositório CRD. Todo cliente suportado pelo Developer for System z e código de host trabalharão com tamanho de registro máximo. Mas o suporte URIMAP estará desativado se o tamanho de registro máximo não for 3000.

## Mensagens do Administrative Utility

As mensagens a seguir são emitidas pelo Administrative utility para a SYSPRINT DD. As mensagens CRAZ1803E, CRAZ1891E, CRAZ1892E e CRAZ1893E contêm códigos de status de arquivo, retorno do VSAM, função do VSAM e feedback do VSAM. Os códigos de retorno, função e feedback do VSAM são documentados em *DFSMS Macro Instructions for Data Sets* (SC26-7408). Os códigos de status de arquivo são documentados em *Enterprise COBOL for z/OS Language Reference* (SC27-1408).

### CRAZ1800I

**concluído com êxito na linha <número da linha da última instrução de controle>**

**Explicação:** O administrative utility do programador de sistema foi concluído com sucesso.

**Resposta do usuário:** Nenhuma.

### CRAZ1801W

**concluído com avisos na linha <número da linha da última instrução de controle>**

**Explicação:** O administrative utility do programador de sistema foi concluído com um ou mais avisos localizados durante o processamento de instruções de controle.

**Resposta do usuário:** Verifique outras mensagens de aviso.

### CRAZ1802E

**encontrado um erro na linha <número da linha>**

**Explicação:** O administrative utility do programador de sistema encontrou um erro grave.

**Resposta do usuário:** Verifique outras mensagens de aviso.

### CRAZ1803E

**Erro ao abrir repositório, status=<código de status do arquivo>  
RC=<código de retorno do VSAM> FC=<código de função do VSAM>  
FB=<código de feedback do VSAM>**

**Explicação:** O administrative utility do programador de sistema encontrou um erro grave ao abrir o repositório do CRD.

**Resposta do usuário:** Verifique os códigos de status, retorno, função e feedback do VSAM.

### CRAZ1804E

**Registro de entrada não reconhecido na linha <número da linha>**

**Explicação:** O administrative utility do programador de sistema encontrou uma instrução de controle de entrada desconhecida.

**Resposta do usuário:** Verifique se o comando **DEFINE** foi seguido por um espaço único e depois pela palavra-chave CPSMNAME, STAGINGGROUPNAME,

MANIFESTEXPORTRULE, DSBINDING, DB2TRAN, DOCTEMPLATE, FILE, MAPSET, PROCESSTYPE, PROGRAM, TDQUEUE ou TRANSACTION.

**CRAZ1805E**

**Processando a palavra-chave <palavra-chave> na linha <número da linha>**

**Explicação:** O administrative utility do programador de sistema está processando a instrução de controle de entrada da palavra-chave DEFINE.

**Resposta do usuário:** Nenhuma.

**CRAZ1806E**

**Regra de exportação de manifesto inválida na linha <número da linha>**

**Explicação:** O administrative utility do programador de sistema encontrou uma regra de exportação de manifesto inválida.

**Resposta do usuário:** Verifique se o valor da palavra-chave MANIFESTEXPORTRULE é "installOnly", "exportOnly" ou "both".

**CRAZ1807E**

**Palavra-chave DSNNAME ausente na linha <número da linha>**

**Explicação:** O administrative utility do programador de sistema estava processando uma instrução de controle DEFINE DSBINDING que não possui a palavra-chave DSNNAME.

**Resposta do usuário:** Verifique se a instrução de controle DEFINE DSBINDING contém a palavra-chave DSNNAME.

**CRAZ1808E**

**Valor inválido da palavra-chave <palavra-chave> na linha <número da linha>**

**Explicação:** O administrative utility do programador de sistema estava processando uma instrução de controle DEFINE e encontrou um valor inválido para a palavra-chave nomeada.

**Resposta do usuário:** Verifique se o comprimento e o valor da palavra-chave nomeada estão corretos.

**CRAZ1890W**

**Erro de sintaxe de palavra-chave na linha <número da linha>**

**Explicação:** O administrative utility do programador de sistema estava processando uma instrução de controle DEFINE e encontrou um erro de sintaxe para a palavra-chave ou valor da palavra-chave.

**Resposta do usuário:** Verifique se o valor da palavra-chave está entre parênteses e imediatamente após a palavra-chave. A palavra-chave e o valor da palavra-chave devem estar contidos na mesma linha.

**CRAZ1891W**

**Erro ao gravar chave duplicada do repositório, status=<código de status do arquivo> RC=<código de retorno do VSAM> FC=<código de função do VSAM> FB=<código de feedback do VSAM>**

**Explicação:** O administrative utility do programador de sistema encontrou um erro de chave duplicada ao gravar no repositório CRD.

**Resposta do usuário:** Verifique os códigos de status, retorno, função e feedback do VSAM.

#### CRAZ1892W

**Erro ao gravar repositório, status=<código de status do arquivo>  
RC=<código de retorno do VSAM> FC=<código de função do VSAM>  
FB=<código de feedback do VSAM>**

**Explicação:** O administrative utility do programador de sistema encontrou um erro grave ao gravar no repositório CRD.

**Resposta do usuário:** Verifique os códigos de status, retorno, função e feedback do VSAM.

#### CRAZ1893W

**Erro ao ler repositório, status=<código de status do arquivo>  
RC=<código de retorno do VSAM> FC=<código de função do VSAM>  
FB=<código de feedback do VSAM>**

**Explicação:** O administrative utility do programador de sistema encontrou um erro grave ao ler o repositório do CRD.

**Resposta do usuário:** Verifique os códigos de status, retorno, função e feedback do VSAM.

---

## Depuração de Transação do CICS

Para depurar transações do CICS, o Depurador Integrado requer as seguintes atualizações do CICS:

- Atualizações do parâmetro de inicialização do sistema CICS (SIT):
  - Especifique DEBUGT00L=YES.
  - Especifique TCPIP=YES.
  - Especifique LLACOPY=YES se você depender do LINKLIST para buscar um módulo de carregamento da concatenação DFHRPL DD.
  - Especifique RENTPGM=NOPROTECT se você não permitir que os usuários usem o Integrated Debugger SVC (necessário para depurar transações carregadas na memória somente de leitura).
- Atualizações de CICS JCL:
  - Especifique REGION=0M na instrução EXEC da região.
  - Defina a biblioteca de carregamento FEK.SFEKAUTH na instrução DFHRPL DD da região. Se o parâmetro SIT LLACOPY=YES for especificado, a biblioteca pode também residir em LINKLIST.
  - Defina a biblioteca de carregamento SYS1.MIGLIB na instrução DFHRPL DD da região. Se o parâmetro SIT LLACOPY=YES for especificado, a biblioteca pode também residir em LINKLIST.
  - Para z/OS 1.13 e superior, defina a biblioteca de carregamento SYS1.SIEAMIGE na instrução DFHRPL DD da região. Se o parâmetro SIT LLACOPY=YES for especificado, a biblioteca pode também residir em LINKLIST.

#### Nota:

- O ID do usuário da região CICS requer permissão UPDATE para o perfil CSVLLA.dataset na classe FACILITY para o parâmetro SIT LLACOPY=YES funcionar conforme projetado.
- Para depurar programas escritos em COBOL v4, o Depurador Integrado precisa acessar um conjunto de dados de listagem (PDS ou PDS/E). O nome do conjunto de dados pode ser fornecido pela variável de ambiente AQE\_DBG\_V4LIST ou DD AQEV4LST. Se nenhuma estiver presente, o Depurador Integrado formará o nome do conjunto de dados substituindo o último

qualificador do conjunto de dados do executável (por exemplo .LOAD) com .LISTING. Pergunte a seus desenvolvedores que método é utilizável em seu site.

- Atualizações de CSD do CICS:

Defina o depurador para uma região do CICS, conforme documentado na tarefa de atualização do CSD de amostra AQECSD. AQECSD está localizado em FEK.#CUST.JCL, a menos que o programador de sistema z/OS tenha especificado um local diferente ao customizar e enviar a tarefa FEK.SFEKSAMP(FEKSETUP). Consulte "Configuração de Customização" no *Guia de Configuração de Host* (SC23-7658) para obter mais detalhes.

Para depurar transações do CICS carregadas na memória de leitura, o Depurador Integrado requer as seguintes atualizações do sistema:

- Chamada do supervisor do Depurador Integrado (SVC) definida para seu sistema. Consulte "Mudanças em PARMLIB" no *Guia de Configuração de Host* (SC23-7658) para obter mais detalhes.
- O SVC requer que os usuários tenham permissão para um perfil de segurança se usado em um ambiente de estado de problema (não autorizado). Consulte "Segurança de Depuração" na página 40 para obter mais detalhes.

**Nota:**

- Somente um depurador baseado no Ambiente de linguagem (LE) pode estar ativo em uma determinada região CICS. Uma indicação clara de um depurador baseado em LE é que ele fornece um módulo de carregamento ou alias CEEEVDBG que deve estar disponível ao aplicativo.
- O Integrated Debugger usa CICS CADP para fornecer opções de tempo de execução TEST para transações CICS. Para obter mais informações em CADP, consulte sua documentação do CICSTS.

---

## Capítulo 9. Considerações da Saída de Usuário

Esse capítulo o ajuda a aprimorar o Developer for System z ao gravar as rotinas de saída.

O Developer for System z fornece pontos de saída para selecionar os eventos do Developer for System z. Um ponto de saída é um ponto específico em um processamento de função no qual a função chama uma rotina de saída, se houver. É possível gravar uma rotina de saída para executar o processamento adicional.

Note que, ao contrário da maioria dos pontos de saída tradicionais, os pontos de saída do Developer for System z não permitem que você altere o comportamento da função. A rotina de saída, se houver, é chamada de forma assíncrona, após a função ser concluída. O processamento do Developer for System z não espera a rotina de saída terminar, nem verifica o status de conclusão.

---

### Características da Saída de Usuário

#### Ativação da Saída de Usuário

As saídas de usuário são ativadas com as variáveis `_RSE_JAVAOPTS` `<exit_point>.action` no `rsed.envvars`, em que `<exit_point>` representa uma palavra-chave que identifica um ponto de saída específico, conforme documentado em “Pontos de Saída Disponíveis” na página 151.

```
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -D<exit_point>.action=<user_exit>"
```

Por padrão, todos os pontos de saída ficam desativados. Remova o comentário e especifique o nome do caminho completo da rotina de saída do usuário para ativar o ponto de saída.

```
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -D<exit_point>.action.id=<userid>"
```

Por padrão, o ID do usuário designado para o daemon RSE é usado para executar a rotina de saída fornecida. Remova o comentário e especifique um ID do usuário para usar o ID especificado para executar a saída de usuário. Não há necessidade de especificar uma senha porque o RSE gerará um PassTicket para ser usado como senha quando ele alternar para o ID do usuário especificado.

#### Gravando uma Rotina de Saída do Usuário

As rotinas de saída do usuário são chamadas como um comando shell z/OS UNIX com possivelmente um ou mais argumentos. Isso significa que a rotina de saída desenvolvida deve ser executável na linha de comandos do z/OS UNIX. As técnicas de codificação comuns incluem o shell script do z/OS UNIX e o REXX `exec` do z/OS UNIX, mas o código compilado como C/C++ também é possível.

Consulte o *Guia do Usuário do UNIX System Services* (SA22-7801) para saber mais sobre os shell scripts do z/OS UNIX. Consulte *Usando REXX e z/OS UNIX System Services* (SA22-7806) para saber mais sobre as extensões específicas do z/OS UNIX para a linguagem REXX.

A rotina de saída provavelmente será executada por um ID do usuário com permissões especiais (como o ID do usuário de tarefa iniciada do RSE, que é



permitido para gerar os PassTickets). Portanto, é importante que você limite a autoridade de atualização para a rotina de saída para evitar abuso. Os limites de comandos de amostra a seguir do z/OS UNIX gravam a autoridade somente para o proprietário, embora todos possam ler e executar o script.

```
$ chmod 755 process_logon.sh
$ ls -l process_logon.sh
-rwxr-xr-x 1 IBMUSER SYS1 2228 Feb 28 23:44 process_logon.sh
```

As definições no `rsed.envvars` estão disponíveis para a rotina de saída do usuário como variáveis de ambiente.

O RSE chama a rotina de saída do usuário com uma sequência de argumentos única. A sequência de argumentos pode ser um valor único ou uma sequência única que retém diversas palavras-chave e valores delimitados em branco. Consulte “Pontos de Saída Disponíveis” na página 151 para obter mais detalhes.

## Mensagens do console

O Developer for System z usa o ID de mensagem do console FEK910I para exibir os dados relacionados às saídas de usuário.

A chamada da rotina de saída é marcada com a mensagem do console a seguir:

```
FEK910I <EXIT_POINT> EXIT: invoking <exit_point> processing exit
in thread <thread_id>
```

Todos os dados gravados no stdout (comando **echo** em um shell script, comando **say** em um REXX exec) serão enviados ao console:

```
FEK910I <EXIT_POINT> EXIT: <message>
```

A terminação da rotina de saída é marcada com a mensagem do console a seguir:

```
FEK910I <EXIT_POINT> EXIT: completed <exit_point> processing exit
in thread <thread_id>
```

## Executando com um ID do Usuário da Variável

O Developer for System z permite executar uma rotina de saída com o ID do usuário de tarefa iniciada ou com um ID do usuário especificado. Entretanto, talvez você queira executar algumas ações na rotina de saída usando outro ID do usuário, como o ID de usuário cliente na rotina de saída do logon. Isso pode ser realizado com o uso dos serviços padrão do z/OS UNIX, conforme mostrado nas amostras a seguir.

### Shell Script do z/OS UNIX

Conforme documentado na *Referência de Comando do UNIX System Services* (SA22-7802), o z/OS UNIX oferece o comando **su** para usar os privilégios de um superusuário ou outro usuário. Há algumas coisas a serem lembradas ao usar o comando **su**.

- O ID do usuário que executa o comando **su** deve ter a permissão READ para o perfil BPX.SRV.<userid> na classe SURROGAT de seu produto de segurança para poder alternar para o ID do usuário identificado pelo <userid> sem especificar uma senha.
- O comando **su** inicia um novo shell, para que os comandos restantes em seu shell script não sejam executados até que o shell iniciado pelo comando **su** saia. Para que os comandos de estágio sejam executados no novo shell iniciado pelo comando **su**, é possível usar o comando **echo** para criar o comando desejado e o caractere do comando de canal para alimentá-lo no novo shell, conforme mostrado no exemplo a seguir. Observe que as regras de criação de shell script padrão se aplicam para os caracteres especiais de escape.

```
#!/bin/sh
myID=ibmuser
echo a ${id}
echo 'echo b ${id}' | su -s $myID
echo "echo c \${id}" | su -s $myID
cat /u/ibmuser/iefbr14
echo "submit /u/ibmuser/iefbr14" | su -s $myID
```

Essa saída de logon de amostra, executada pelo ID do usuário de tarefa iniciada, resultará nas mensagens de console a seguir:

```
+FEK910I LOGON EXIT: invoking logon processing exit in thread 411
+FEK910I LOGON EXIT: a uid=8(STCRSE) gid=1(STCGRP)
+FEK910I LOGON EXIT: b uid=1(IBMUSER) gid=0(SYS1)
+FEK910I LOGON EXIT: c uid=1(IBMUSER) gid=0(SYS1)
+FEK910I LOGON EXIT: //IEFBR14 JOB CLASS=A,MSGCLASS=A,MSGLEVEL=(1,1)
+FEK910I LOGON EXIT: //IEFBR14 EXEC PGM=IEFBR14
$HASP100 IEFBR14 ON INTRDR FROM STC03919
IBMUSER
IRR010I USERID IBMUSER IS ASSIGNED TO THIS JOB.
+FEK910I LOGON EXIT: JOB JOB03926 submitted from path '/u/ibmuser/iefbr14'
ICH70001I IBMUSER LAST ACCESS AT 00:46:13 ON MONDAY, MARCH 19, 2012
$HASP373 IEFBR14 STARTED - INIT 2 - CLASS A - SYS CD08
IEF403I IEFBR14 - STARTED - TIME=00.46.14
+FEK910I LOGON EXIT: completed logon processing exit in thread 411
IEFBR14 IEFBR14 IEFBR14 0000
IEF404I IEFBR14 - ENDED - TIME=00.46.14
$HASP395 IEFBR14 ENDED
$HASP309 INIT 2 INACTIVE ***** C=BA
```

## REXX exec do z/OS UNIX

Conforme documentado em *Usando REXX e z/OS UNIX System Services*

(SA22-7806), o z/OS UNIX oferece o comando **seteuaid** SYSCALL para configurar o UID efetivo do processo atual. Há algumas coisas a serem lembradas ao usar o comando **seteuaid**.

- O comando **seteuaid** usa o UID do z/OS UNIX, não o ID do usuário MVS. Você deve primeiramente determinar o UID do ID do usuário de destino, o que pode ser feito com o comando **getpwnam** SYSCALL.
- O ID do usuário que executa o comando **seteuaid** deve ter a permissão READ para o perfil BPX.SRV.<userid> na classe SURROGAT de seu produto de segurança para poder alternar para o ID do usuário identificado pelo <userid> sem especificar uma senha. Observe que, quando diversos IDs do usuário compartilham o mesmo UID, não há um modo de determinar qual deles será verificado.

```
/* rexx */
myID='ibmuser'
say userid()
address SYSCALL 'getpwnam' myID 'pw.'
say pw.1 pw.2 pw.3 pw.4 pw.5
address SYSCALL 'seteuaid' pw.2 /* PW_UID = 2 */
say retval errno errnojr
say userid()
```

Essa saída de logon de amostra, executada pelo ID do usuário de tarefa iniciada, resultará nas mensagens de console a seguir:

```
+FEK910I LOGON EXIT: invoking logon processing exit in thread 515
+FEK910I LOGON EXIT: STCRSE
+FEK910I LOGON EXIT: IBMUSER 1 0 /bin/sh
+FEK910I LOGON EXIT: 0 0 0
+FEK910I LOGON EXIT: IBMUSER
+FEK910I LOGON EXIT: completed logon processing exit in thread 515
```

## Pontos de Saída Disponíveis

Os pontos de saída a seguir são fornecidos pelo Developer for System z:

- “audit.action”
- “logon.action” na página 152

### audit.action

- Sincronização:

A saída de usuário de auditoria é chamada quando o arquivo de log de auditoria ativo é fechado. (A auditoria continua como RSE alternada para um novo arquivo de log de auditoria.)

- **Argumentos de chamada (1):**

- <audit\_log>: nome do caminho completo do arquivo de log de auditoria que foi encerrado

- **Amostra:**

`/usr/lpp/rdz/samples/process_audit.rex`

Essa amostra z/OS UNIX REXX exec constrói uma tarefa em lote que processará o log de auditoria que foi encerrado.

## logon.action

- **Sincronização:**

A saída de usuário do logon é chamada quando um usuário tiver concluído o processo de logon.

- **Argumentos de chamada (6):**

- -i <userid>: ID de usuário cliente, maiúsculas e minúsculas conforme fornecido pelo cliente
- -u <user\_log\_path>: diretório no qual os logs de usuário desse cliente são mantidos
- -s <server\_log\_path>: diretório no qual os logs do servidor são mantidos
- -c <config\_path>: diretório no qual os arquivos de configuração são mantidos
- -b <binaries\_path>: diretório no qual o Developer for System z está instalado
- -p <port>: porta daemon RSE

- **Amostra:**

`/usr/lpp/rdz/samples/process_logon.sh`

Esse shell script do z/OS UNIX de amostra grava uma mensagem de logon no console.

---

## Capítulo 10. Customizando o Ambiente TSO

Este capítulo é fornecido para auxiliar a imitar um procedimento de logon de TSO incluindo instruções DD e conjuntos de dados no ambiente do TSO em Developer for System z.

---

### O Serviço TSO Commands

O serviço TSO Commands é o componente Developer for System z que executa comandos TSO e ISPF (em lote) e retorna o resultado para o cliente solicitante. Esses comandos podem ser solicitados implicitamente pelo produto ou explicitamente pelo usuário.

Os membros de amostra fornecidos com o Developer for System z criam um ambiente mínimo do TSO/ISPF. Se os desenvolvedores em sua loja precisarem de acesso a bibliotecas customizadas ou de terceiros, o programador de sistema z/OS deve incluir as instruções DD e as bibliotecas necessárias para o ambiente de serviço TSO Commands. Embora a implementação seja diferente no Developer for System z, a lógica por trás disso é idêntica ao procedimento de logon do TSO.

**Nota:** O serviço TSO Commands é uma ferramenta de linha de comandos não interativa, portanto, os comandos ou procedimentos que solicitam dados ou exibem painéis ISPF não funcionarão. Um emulador 3270, como o Host Connect Emulator que faz parte do cliente Developer for System z, será necessário para executá-los.

### Métodos de Acesso

A partir da versão 7.1, o Developer for System z fornece uma opção para acessar o serviço TSO Commands.

- O serviço de Gateway do Cliente TSO/ISPF do ISPF, que requer um nível mínimo de serviço do ISPF. Este é o método padrão usado nas amostras fornecidas.
- Uma transação APPC (como em releases pré-versão 7.1). Este método é reprovado.

**Nota:**

- O serviço de Gateway do Cliente TSO/ISPF do ISPF substitui a função do SCLM Developer Toolkit usada na versão 7.1.
- O uso de APPC por Developer for System z está marcado como reprovado. As informações relacionadas ao APPC foram removidas desta publicação. Para obter mais informações, consulte o White Paper *Using APPC to provide TSO command services* (SC14-7291), disponível na biblioteca do Developer for System z, <http://www-01.ibm.com/support/docview.wss?uid=swg27038517>.

Verifique o `rsed.envvars` para determinar qual método de acesso é usado para hosts da versão 7.1 e superior. Se os padrões tiverem sido usados durante o processo de configuração, `rsed.envvars` residirá em `/etc/rdz/`.

- Se a instrução `_RSE_JAVAOPTS="$_RSE_JAVAOPTS -DTSO_SERVER=APPC"` não estiver presente (ou for uma linha comentada), o serviço de Gateway do Cliente TSO/ISPF do ISPF será usado.

- Se a instrução `_RSE_JAVAOPTS="$_RSE_JAVAOPTS -DTSO_SERVER=APPC"` estiver presente (e não estiver assinalada como comentário), o APPC será usado.

## Usando o Método de Acesso do TSO/ISPF Client Gateway

### ISPF.conf

O arquivo de configuração ISPF.conf (localizado por padrão em /etc/rdz/) define o ambiente do TSO/ISPF usado pelo Developer for System z. Existe apenas um arquivo de configuração ISPF.conf ativo, que é usado por todos os usuários do Developer for System z.

A seção principal do arquivo de configuração define os nomes DD e as concatenações relacionadas do conjunto de dados, como no seguinte exemplo:

```
sysproc=ISP.SISPLIB,FEK.SFEKPROC
ispmlib=ISP.SISPMENU
isptlib=ISP.SISPTENU
ispplib=ISP.SISPPENU
ispslib=ISP.SISPSLIB
ispllib=ISP.SISPLOAD
myDD=HLQ1.LLQ1,HLQ2.LLQ2
```

- Cada definição de DD utiliza exatamente uma linha (não há suporte para várias linhas) e não existem limites de comprimento de linha.
- As definições não fazem distinção entre maiúsculas e minúsculas e qualquer espaço em branco será ignorado.
- As linhas de comentário iniciam com um asterisco (\*).
- Os nomes DD são seguidos por um sinal de igual (=), que por sua vez é seguido pela concatenação do conjunto de dados. Vários nomes de conjunto de dados são separados por uma vírgula (,).
- As concatenações do conjunto de dados são procuradas na ordem em que são listadas.
- Os conjuntos de dados devem ser completos, sem ser colocados entre aspas (') e sem o uso de variáveis.
- Todos os conjuntos de dados são alocados com `DISP=SHR`.
- Novos nomes DD podem ser incluídos à vontade, mas devem obedecer as regras (JCL) para nomes DD e não podem ser conflitantes com outros parâmetros de configuração no ISPF.conf. Além disso, o ISPPROF é alocado dinamicamente (`DISP=NEW,DELETE`) pelo serviço TSO/ISPF Client Gateway.

### Usar Perfis do ISPF Existentes

Por padrão, o TSO/ISPF Client Gateway cria um perfil temporário do ISPF para o serviço TSO Commands. Entretanto, você pode instruir o TSO/ISPF Client Gateway a utilizar uma cópia de um perfil existente do ISPF. A chave aqui é a instrução `_RSE_ISPF_OPTS` em `rsed.envvars`.

```
#_RSE_ISPF_OPTS="$_RSE_ISPF_OPTS&ISPPROF=&SYSUID..ISPPROF"
```

Remova o comentário da instrução (remova o sinal de sustenido (#) inicial) e forneça o nome completo do conjunto de dados do perfil existente do ISPF para utilizar esse recurso.

As seguintes variáveis podem ser usadas no nome do conjunto de dados:

- `&SYSUID`. para substituir o ID do usuário do desenvolvedor
- `&SYSPREF`. para substituir o prefixo do TSO do desenvolvedor
- `&SYSNAME`. para substituir o nome do sistema conforme especificado no membro da parmlib IEASYMxx

**Nota:**

- Se o nome do conjunto de dados transmitido em "ISPPROF" for inválido, um perfil de ISPF vazio temporário será usado.
- O perfil do ISPF (temporário e copiado) é excluído no final da sessão. As alterações feitas no perfil não são mescladas com o perfil existente do ISPF.

## Usando um exec de alocação

A instrução `allocjob` no `ISPF.conf` (que está assinalada como comentário por padrão) aponta um exec que pode ser usado para fornecer alocações adicionais do conjunto de dados por ID do usuário.

```
*allocjob = ISP.SISPSAMP(ISPZISP2)
```

Remova o comentário da instrução (remova o caractere de asterisco (\*) inicial) e forneça a referência completa para o exec de alocação para utilizar esse recurso.

- O exec é executado após a alocação de ISPPROF e os DDs definidos em `ISPF.conf`, mas antes de o ISPF ser inicializado. Assegure-se de que o exec de alocação não desfaça essas definições.
- 1 parâmetro é transmitido ao exec; o ID do usuário do responsável pela chamada.
- Um exec de amostra `CRAISPRX` é fornecido na biblioteca de amostra `FEK.#CUST.CNTL`, a menos que você tenha especificado um local diferente quando customizou e enviou a tarefa `FEK.SFEKSAMP(FEKSETUP)`. Consulte "Configuração de customização" no *Guia de Configuração do Host* (SC23-7658) para obter mais detalhes.

**Nota:** Como o exec é chamado antes do ISPF ser inicializado, você não pode utilizar `VPUT` e `VGET`. No entanto, você pode criar suas próprias implementações dessas funções utilizando um arquivo VSAM ou PDS(E).

## Usar Diversos Execs de Alocação

Embora o `ISPF.conf` suporte apenas a chamada de um exec de alocação, não há limites para um exec chamar outro exec. E o ID do usuário do cliente que está sendo transmitido como parâmetro abre os execs de alocação personalizados. Você pode, por exemplo, verificar se o membro `USERID'.EXEC(ALLOC)'` existe e executá-lo.

Uma variação elaborada para esse tema permite o uso de procedimentos de logon existentes do TSO, como a seguir:

- Leia um arquivo de configuração específico do usuário, como `USERID'.FEKPROF'`.
- Consulte qual procedimento de logon é mencionado no arquivo.
- Leia o procedimento mencionado a partir de `SYS1.PROCLIB` e analise-o para localizar as instruções DD e as alocações de conjunto de dados contidas.
- Aloque o conjunto de dados de uma forma semelhante ao procedimento de logon real.

## Diversos Arquivos ISPF.conf com Diversas Configurações do Developer for System z

Se os cenários de exec de alocação descritos nas seções anteriores não puderem tratar de suas necessidades específicas, você poderá criar instâncias diferentes do servidor de comunicação RSE do Developer for System z, cada uma delas usando seu próprio arquivo `ISPF.conf`. A desvantagem principal do método descrito a

seguir é que os usuários do Developer for System z devem conectar-se a servidores diferentes no mesmo host para obter o ambiente TSO desejado.

**Nota:** A criação de uma segunda instância do servidor RSE requer apenas a duplicação e atualização de arquivos de configuração, JCL de inicialização e definições de tarefa iniciada. Não é necessária uma nova instalação do produto e nenhum código é duplicado.

```
$ cd /etc/rdz
$ mkdir /etc/rdz/tso2
$ cp rsed.envvars /etc/rdz/tso2
$ cp ISPF.conf /etc/rdz/tso2
$ ls /etc/rdz/tso2
ISPF.conf rsed.envvars
$ oedit /etc/rdz/tso2/rsed.envvars
-> change: _RSE_RSED_PORT=4037
-> change: CGI_ISPCONF=/etc/rdz/tso2
-> change: -Ddaemon.log=/var/rdz/logs/tso2
-> change: -Duser.log=/var/rdz/logs/tso2
-> add at the END:
-- NEEDED TO FIND THE REMAINING CONFIGURATION FILES
CFG_BASE=/etc/rdz
CLASSPATH=.:$CFG_BASE:$CLASSPATH
--
$ oedit /etc/rdz/tso2/ISPF.conf
-> change: change as needed
```

Os comandos no exemplo anterior copiam os arquivos de configuração do Developer for System z que exigem alterações no diretório tso2 recém-criado. A variável CGI\_ISPCONF em rsed.envvars deve ser atualizada para definir o novo diretório inicial ISPF.conf, e daemon.log e user.log devem ser atualizados para definir um novo local de log (que é criado automaticamente se não existir). A atualização \_RSE\_RSED\_PORT assegura que o daemon do RSE existente e novo usarão números de porta exclusivos. A atualização de CLASSPATH assegura que o RSE possa localizar os arquivos de configuração que não foram copiados para tso2. O arquivo ISPF.conf em si pode ser atualizado para atender às suas necessidades. Observe que a área de trabalho do ISPF (variável CGI\_ISPWORK em rsed.envvars) pode ser compartilhada entre ambas as instâncias.

Agora resta apenas criar uma nova tarefa iniciada para o RSE que utiliza um novo número de porta e os novos arquivos de configuração /etc/rdz/tso2. Observe que se \_RSE\_RSED\_PORT não for alterado em rsed.envvars, a nova tarefa iniciada deverá especificar uma nova porta como argumento de inicialização.

Consulte o *Guia de Configuração de Host do IBM Rational Developer for System z* (SC23-7658) para obter mais informações sobre as ações mostradas anteriormente nesta seção.



---

## Capítulo 11. Executando várias instâncias

Há situações em que você deseja várias instâncias do Developer for System z ativas no mesmo sistema, por exemplo, durante o teste de um upgrade. Entretanto, alguns recursos, como portas TCP/IP, não podem ser compartilhadas, portanto os padrões nem sempre são aplicáveis. Use as informações nessa seção para planejar a coexistência de instâncias diferentes do Developer for System z, após é possível usar esse guia de configuração para customizá-las.

Embora seja possível compartilhar certas partes do Developer for System z entre duas (ou mais) instâncias, isso NÃO é recomendado, a menos que seus níveis de software sejam idênticos e as únicas alterações sejam nos membros de configuração. O Developer for System z deixa espaço de customização suficiente para criar várias instâncias que não se sobrepõem, e recomendamos a utilização destes recursos.

### Nota:

- FEK e /usr/lpp/rdz são o qualificador de alto nível e o caminho usados durante a instalação do produto. FEK.#CUST, /etc/rdz e /var/rdz são os locais padrão usados durante a customização do produto (consulte "Configuração de customização" no *Guia de Configuração do Host* (SC23-7658) para obter informações adicionais)..
- Você deve instalar o Developer for System z em um sistema de arquivos privado (HFS ou zFS) para facilitar a implementação das partes do produto z/OS UNIX.
- Se você não puder usar um sistema de arquivos privado, deverá usar uma ferramenta de arquivamento, como o comando z/OS UNIX tar para transportar os diretórios do z/OS UNIX de sistema para sistema. Isso para preservar os atributos (como controle de programas) para os arquivos e diretórios do Developer for System z.

Consulte *UNIX System Services Command Reference* (SA22-7802) para obter informações adicionais sobre os seguintes comandos de amostra para arquivar e restaurar o diretório de instalação do Developer for System z.

- Archive: `cd /SYS1/usr/lpp/rdz; tar -cSf /u/userid/rdz.tar`
- Restore: `cd /SYS2/usr/lpp/rdz; tar -xSf /u/userid/rdz.tar`

---

## Configuração idêntica em um sysplex

Os arquivos de configuração do Developer for System z (e código) podem ser compartilhados entre diferentes sistemas em um sysplex, com cada sistema executando sua própria cópia idêntica do Developer for System z, se algumas diretrizes forem obedecidas. Observe que estas informações destinam-se a instâncias do Developer for System z independentes. Regras adicionais para a configuração do TCP/IP são aplicadas usando o Distributed Dynamic VIPA para agrupar diversos servidores (cada qual em um sistema separado) em um servidor virtual, conforme documentado em "Distributed Dynamic VIPA" na página 65.

- Os arquivos de log devem terminam em locais únicos para impedir que um sistema sobrescreva as informações de outro. Ao rotear os logs do z/OS UNIX para especificar locais com as diretivas `daemon.log` e `user.log` em `rsed.envvars`, é possível compartilhar os arquivos de configuração se montar um sistema de arquivos z/OS UNIX específico do sistema no caminho especificado. Dessa

maneira, todos os logs são gravados no mesmo local lógico, mas devido ao sistema de arquivos não compartilhado abaixo, eles terminam em locais físicos diferentes.

- Os diretórios do tipo configuração, como /etc/rdz/ e /var/rdz/pushtoclient/, podem ser compartilhados entre o sysplex, como o Developer for System z os usa em modo somente leitura.
- Diretórios de dados temporários como /tmp/ e /var/rdz/WORKAREA/ devem ser exclusivos por sistema, uma vez que os nomes de arquivos temporários não são preparados para sysplex.
- Se você compartilhar o código, deverá compartilhar também os arquivos de configuração para garantir que não tenha alguns sistemas fora de sincronização depois de aplicar manutenção.
- Se você compartilhar um arquivo de configuração ativo /etc/rdz/pushtoclient.properties, deverá compartilhar também o diretório de metadados relacionado, /var/rdz/pushtoclient/.

---

## Arquivos de Configuração Diferentes de Níveis de Software Idênticos

Em algum conjunto limitado de circunstâncias, é possível compartilhar tudo, menos (algumas das) as partes customizáveis. Um exemplo é fornecer acesso não SSL para uso no site e comunicação codificada por SSL para uso externo.

**Atenção:** A configuração compartilhada NÃO PODE ser usada com segurança para manutenção de teste, visualização técnica ou novo release.

Para configurar outra instância de uma instalação ativa do Developer for System z, refaça as etapas de customização das partes que são diferentes, usando conjuntos de dados, diretórios e portas diferentes para evitar sobreposição da configuração atual.

Na amostra de SSL mencionada anteriormente, a configuração do daemon RSE atual pode ser fechada e depois a configuração clonada pode ser atualizada. Em seguida, a JCL de inicialização do daemon RSE pode ser clonada e customizada com uma nova porta TCP/IP e o local dos arquivos de configuração atualizado. As customizações MVS (JES Job Monitor, entre outras) podem ser compartilhadas entre instâncias SSL e não SSL. Isso resultaria nas seguintes ações:

```
$ cd /etc/rdz
$ mkdir /etc/rdz/ssl
$ cp rsed.envvars /etc/rdz/ssl
$ cp ssl.properties /etc/rdz/ssl
$ ls /etc/rdz/ssl/
rsed.envvars ssl.properties
$ oedit /etc/rdz/ssl/rsed.envvars
-> change: RSE_RSED_PORT=4047
-> change: -Ddaemon.log=/var/rdz/logs/ssl
-> change: -Duser.log=/var/rdz/logs/ssl
-> add at the END:
-- NEEDED TO FIND THE REMAINING CONFIGURATION FILES
CFG_BASE=/etc/rdz
CLASSPATH=.:$CFG_BASE:$CLASSPATH
--
$ oedit /etc/rdz/ssl/ssl.properties
-> change: change as needed
```

Os comandos no exemplo anterior copiam os arquivos de configuração do Developer for System z que requerem mudanças em um diretório recém-criado ssl. As variáveis daemon.log e user.log em rsed.envvars devem ser atualizadas para definir um novo local de log (o qual será criado automaticamente se ainda não existir). A atualização de CLASSPATH assegura que o RSE possa localizar os arquivos de configuração que não foram copiados para ssl. O próprio arquivo ssl.properties pode ser atualizado para corresponder às suas necessidades.

Agora resta criar uma nova tarefa iniciada para o RSE que usa um novo número de porta e os novos arquivos de configuração /etc/rdz/ssl.

Consulte as seções relacionadas no *Guia de Configuração do HostIBM Rational Developer for System z (SC23-7658)* para obter mais informações sobre as ações mostradas anteriormente nesta seção.

**Nota:** Ao usar esta técnica para criar clones dependentes, saiba que `ssl.properties` deve ser sempre clonado para o diretório dependente, mesmo que ele não seja alterado. `rsed.envvars` Deve também ser copiado e, pelo menos a diretiva `_RSE_RSED_PORT` deve ser alterada.

## Sincronização Automatizada

Na amostra de SSL mencionada anteriormente, as mudanças entre o daemon RSE ativado por SSL e não SSL são mínimas, o que permite automatizar o processo de manter seus arquivos `rsed.envvars` sincronizados. Isso simplifica o lançamento de serviço porque apenas um arquivo `rsed.envvars` deve ser mantido.

O exemplo a seguir inclui um número da porta RSED nos nomes do diretório de log e atualiza o CLASSPATH para que os clones localizem o restante dos arquivos de configuração. Em seguida, o exemplo melhora a tarefa JCL iniciada do daemon RSE ativado por SSL para clonar o `rsed.envvars` do daemon RSE não SSL na inicialização, atualizando o número da porta no processo. Como o número da porta é integrado no nome do diretório de log, ele será automaticamente diferente entre os dois daemons.

### 1. Prepare o `rsed.envvars` principal.

```
$ oedit /etc/rdz/rsed.envvars
-> change: -Ddaemon.log=/var/rdz/logs/$RSE_RSED_PORT
-> change: -Duser.log=/var/rdz/logs/$RSE_RSED_PORT
-> add at the END:
-- NEEDED BY CLONES TO FIND THE REMAINING CONFIGURATION FILES
CFG_BASE=/etc/rdz
CLASSPATH=.:$CFG_BASE:$CLASSPATH
--
```

### 2. Prepare outros arquivos de configuração (que não são arquivos `rsed.envvars`) que diferem entre o principal (não SSL) e o clone (SSL).

```
$ mkdir /etc/rdz/ssl
$ cp /etc/rdz/ssl.properties /etc/rdz/etc/rdz/ssl
$ oedit /etc/rdz/ssl/ssl.properties
-> change: change as needed
```

### 3. Crie uma tarefa iniciada RSED que clone o `rsed.envvars` de base e altere a porta do daemon RSE (4035 -> 4034).

```
/*
/* RSE DAEMON - SSL
/*
//RSED PROC IVP=, * 'IVP' to do an IVP test
// HOME='/usr/lpp/rdz',
// CNFG='/etc/rdz/ssl'
/*
// SET SED="/RSED_PORT/s/4035/4034/"
// SET FILE='rsed.envvars'
/*
/* copy /etc/rdz/rsed.envvars to /etc/rdz/ssl/rsed.envvars
/* and alter RSED_PORT
/*
//CLONE EXEC PGM=BPXBATCH,REGION=0M,COND=(4,LT),
// PARM='SH cd &CNFG;sed &SED ../&FILE>&FILE'
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
/*
/* start RSED with the newly created rsed.envvars
/*
//RSED EXEC PGM=BPXBATCH,REGION=0M,TIME=NOLIMIT,COND=(4,LT),
// PARM='PGM &HOME./bin/rsed.sh IVP -C&CNFG'
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
// PEND
/*
```

---

## Todas as Outras Situações

Quando alterações de código estiverem envolvidas (manutenção, visualizações técnicas, novo release), ou suas alterações forem razoavelmente complexas, é aconselhável fazer outra instalação do Developer for System z. Esta seção descreve os possíveis pontos de conflito entre as diferentes instalações.

A lista a seguir é uma breve visão geral dos itens que devem ser ou são altamente aconselhados a serem diferentes entre as instâncias do Developer for System z:

- SMP/E CSI
- Bibliotecas de instalação
- Porta TCP/IP do JES Job Monitor e seu arquivo de configuração FEJJCNFG
- JCL de inicialização do JES Job Monitor
- Nome da transação APPC
- Arquivos de configuração RSE, rsed.envvars, \*.properties e \*.conf
- Porta TCP/IP do RSE
- JCL de inicialização do RSE

Uma visão geral mais detalhada é listada a seguir:

- SMP/E CSI
  1. Instale cada instância do Developer for System z em um CSI separado. O SMP/E evitará uma segunda instalação do mesmo FMID em um CSI, mas aceitará a instalação de outro FMID. Se o segundo FMID for de uma versão mais recente, ele excluirá a versão existente do produto. Se o segundo FMID for de uma versão mais antiga, a instalação falhará devido a nomes de partes duplicados.
- Bibliotecas de instalação
  1. Instale cada instância do Developer for System z em conjuntos de dados e diretórios separados. Lembre-se de que você só pode alterar o caminho do z/OS UNIX prefixando o padrão /usr/lpp/rdz fornecido pela IBM. Uma amostra válida seria /service/usr/lpp/rdz.
  2. A tarefa de configuração de customização FEK.SFEKSAMP(FEKSETUP) cria os conjuntos de dados e diretórios usados para armazenar arquivos de configuração. Como os arquivos de configuração devem ser exclusivos, e para evitar sobrescrever customizações existentes, você deve utilizar nomes de conjuntos de dados e de diretórios exclusivos ao enviar essa tarefa.
- Partes obrigatórias
  1. O arquivo de configuração do JES Job Monitor FEK.#CUST.PARMLIB(FEJJCNFG) contém o número de porta TCP/IP do JES Job Monitor e, portanto, não pode ser compartilhado. O membro pode ser renomeado (se a JCL também for atualizada), portanto você pode colocar todas as versões customizadas deste membro no mesmo conjunto de dados se não estiver realizando as atualizações no conjunto de dados da instalação.
  2. A JCL de inicialização do JES Job Monitor FEK.#CUST.PROCLIB(JMON) refere-se a FEJJCNFG e, portanto, também não pode ser compartilhada. Depois de renomear o membro (e o cartão JOB, se você iniciá-lo como uma tarefa do usuário), todas as JCLs poderão ser colocadas no mesmo conjunto de dados.
  3. O arquivo de configuração RSE /etc/rdz/rsed.envvars contém referências para o caminho de instalação e, opcionalmente, para o local do log do servidor, que requer que ela seja exclusivo. O nome do arquivo é obrigatório, portanto você não pode manter as cópias diferentes no mesmo diretório.

4. O arquivo de configuração ISPF.conf possui uma referência ao FEK.SFEKPROC. Isto é específico do nível do software, portanto, você deve criar um arquivo ISPF.conf por instância.
  5. Todos os outros arquivos de configuração baseados em z/OS UNIX (como \*.properties) devem residir no mesmo diretório que o rsed.envvars e, portanto, não podem ser compartilhados, uma vez que o rsed.envvars deve estar em um local não compartilhado.
  6. A JCL de inicialização do RSE FEK.#CUST.PROCLIB(RSED) não pode ser compartilhada, já que ela define o número da porta TCP/IP e tem uma referência para os diretórios de instalação e configuração, que devem ser exclusivos. Depois de renomear o membro (e o cartão JOB, se você iniciá-lo como uma tarefa do usuário), todas as JCLs poderão ser colocadas no mesmo conjunto de dados.
- Partes opcionais
    1. As portas TCP/IP do REXEC e do SSH podem ser compartilhadas sem qualquer restrição.
    2. A transação APPC tem uma referência a FEK.SFEKPROC(FEKFRRSV), o servidor TSO Commands. Isto é específico ao nível do software, portanto, você deve criar uma transação APPC por instância. Lembre-se de que, como o nome da transação APPC é alterado, a variável \_FEKFSCMD\_TP\_NAME\_ deve ser definida em rsed.envvars.
    3. Alguns procedimentos ELAXF\* tem uma referência ao FEK.SFEKLOAD, ou FEK.SFEKAUTH, as bibliotecas de carregamento do Developer for System z. Consulte a nota sobre JCLLIB em "Procedimentos de construção remota ELAXF\*" no *Guia de Configuração do Host* (SC23-7658) para obter uma possível solução para disponibilizar conjuntos diferentes aos usuários.
    4. O suporte bidirecional em regiões do CICS depende de um membro da biblioteca de carregamento e, assim, não pode ser compartilhado entre os releases. No entanto, se o nome do módulo de carregamento for idêntico para todas as instâncias, você poderá compartilhar a versão mais recente entre as instâncias, entre os releases. A compatibilidade com versões anteriores não estará disponível se o nome do módulo de carregamento for alterado.
    5. Os módulos de carregamento do Application Deployment Manager que são incluídos nas regiões do CICS têm compatibilidade com versões anteriores e, portanto, a versão mais recente poderá ser compartilhada entre os releases.
    6. O Application Deployment Manager CRD VSAM é compatível com versões anteriores e, portanto, a versão mais recente pode ser compartilhada entre os releases.
    7. As definições de recursos CICS do Application Deployment Manager são compatíveis com versões anteriores e, portanto, a versão mais recente pode ser compartilhada entre os releases.
    8. Os CARMA VSAMs poderiam ser alterados entre os níveis de software, portanto, não é aconselhável compartilhá-los.
    9. A tarefa iniciada do Debug Manager é compatível com versões anteriores e, portanto, a versão mais recente pode ser compartilhada entre as liberações.



---

## Capítulo 12. Resolução de problemas de configuração

Este capítulo é fornecido para ajudá-lo com alguns problemas comuns que você pode encontrar durante a configuração do seu Developer for System z, e possui as seções a seguir:

- “Análise de Log e Configuração Usando FEKLOGS”
- “Arquivos de Log” na página 164
- “Arquivos de dump” na página 170
- “Rastreio” na página 172
- “Bits de permissão do z/OS UNIX” na página 174
- “Portas TCP/IP reservadas” na página 177
- “Tamanho do espaço de endereço” na página 179
- “Informações Variadas” na página 180

A publicação *Developer for System z Messages and Codes* (SC14-7497) documenta mensagens e códigos de retorno gerados por componentes do Developer for System z. *Developer for System z Answers to common host configuration and maintenance issues* (SC14-7373) descreve vários cenários de problemas e sua resolução.

Mais informações estão disponíveis na seção Suporte do website do Developer for System z (<http://www-03.ibm.com/software/products/us/en/developerforsystemz/>), onde é possível localizar as Notas Técnicas que trazem as informações mais recentes de nossa equipe de suporte.

Na seção Biblioteca do website (<http://www-01.ibm.com/support/docview.wss?uid=swg27038517>), também é possível localizar a versão mais recente da documentação do Developer for System z, incluindo White Papers.

O Centro de Informações do Developer for System z ([http://www-01.ibm.com/support/knowledgecenter/SSQ2R2\\_9.1.0/com.ibm.etools.getstart.wsentdev.doc/kc\\_version\\_welcome\\_rdz.html](http://www-01.ibm.com/support/knowledgecenter/SSQ2R2_9.1.0/com.ibm.etools.getstart.wsentdev.doc/kc_version_welcome_rdz.html)) documenta o cliente Developer for System z e como o mesmo interage com o host (de uma perspectiva do cliente).

Informações sobre valor também podem ser localizadas na biblioteca do z/OS na Internet, disponível em <http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/>.

Notifique-nos se pensar que o Developer for System z não tem uma certa função. Você pode abrir uma Solicitação para Aprimoramento (RFE) em

<https://www.ibm.com/developerworks/support/rational/rfe/>

---

### Análise de Log e Configuração Usando FEKLOGS

A tarefa de iniciação do RSED suporta o comando do operador **MODIFY LOGS** para coletar logs de host e informações de configuração do Developer for System z. Os dados coletados são colocados em um arquivo z/OS UNIX, `$TMPDIR/feklogs.%sysname.%jobname`, em que `$TMPDIR` é o valor da diretiva `TMPDIR` in `rsed.envvars` (/tmp padrão), `%sysname` é seu nome do sistema z/OS e `%jobname` é o nome da tarefa iniciada do RSED.



Por padrão, apenas os logs do servidor são coletados. As opções de comando permitem coletar logs diferentes:

|          |                                                              |
|----------|--------------------------------------------------------------|
| USER     | Colete arquivos de logs para os IDs de usuário especificados |
| AUDIT    | Colete logs de auditoria                                     |
| NOSERVER | Não colete logs do servidor                                  |

Developer for System z consultará seu produto de segurança para as permissões de acesso dos perfis do FEK.CMD.LOGS.\*\* a fim de determinar se ao solicitante é permitido coletar os logs especificados. Por padrão, o solicitante é o ID do usuário da tarefa iniciada do RSED, a menos que a opção OWNER seja especificada. Apenas o solicitante possui acesso ao arquivo que está mantendo os dados coletados.

Para coletar dados antes que a tarefa iniciada do RSED possa iniciar, o Developer for System z fornece uma tarefa de amostra, FEKLOGS, que reúne todos os arquivos de log z/OS UNIX, bem como as informações de instalação e configuração do Developer for System z.

A tarefa de amostra FEKLOGS está localizada em FEK.#CUST.JCL, a menos que você tenha especificado um local diferente quando customizou e enviou a tarefa FEK.SFEKSAMP(FEKSETUP). Consulte "Configuração de customização" no *Guia de Configuração do Host* (SC23-7658) para obter mais detalhes.

A customização de FEKLOGS é descrita dentro da JCL. A customização inclui a provisão de algumas variáveis principais.

**Nota:** Os clientes do SDSF podem usar o comando da linha XDC no SDSF para salvar a saída da tarefa em um conjunto de dados, o qual, por sua vez, pode ser fornecido para o centro de suporte IBM. Observe que o conjunto de dados de saída deve ser alocado como VB 2051 (o valor padrão no SDSF é VB 240) para evitar truncamento de registro.

---

## Arquivos de Log

O Developer for System z cria arquivos de log que podem auxiliar você e o centro de suporte da IBM na identificação e solução de problemas. A lista a seguir é uma visão geral de arquivos de log que podem ser criados no sistema host do z/OS. Ao lado desses logs específicos do produto, assegure-se de marcar o SYSLOG de todas as mensagens relacionadas.

Os logs baseados no MVS podem ser localizados na instrução DD apropriada. Arquivos de log baseados no z/OS UNIX estão localizados nos seguintes diretórios:

- userlog/\$LOGNAME/

Os arquivos de log específicos do usuário estão localizados em userlog/\$LOGNAME/, em que userlog é o valor combinado das diretivas user.log e DSTORE\_LOG\_DIRECTORY em rsed.envvars, e \$LOGNAME é o ID do usuário de logon (em maiúsculas). Se a diretiva user.log for comentada ou não estiver presente, o caminho inicial do usuário será usado. O caminho inicial é definido no segmento de segurança OMVS do ID de usuário. Se a diretiva DSTORE\_LOG\_DIRECTORY for comentada ou não estiver presente, então .eclipse/RSE/ será anexado ao valor user.log.

- .dstoreMemLogging - Criação de log de uso de memória do armazenamento de dados
- .dstoreTrace - Criação de log de ação do armazenamento de dados
- .dstoreHashmap.\* - captura instantânea do hasmap do DataStore ativo
- .dstoreStackTrace.\* - captura instantânea dos encadeamentos do DataStore ativo e onde eles são chamados
- ffs.log - O log do servidor Foreign File System (FFS), que executa funções MVS nativas
- ffsget.log - O log do leitor de arquivos, que lê um conjunto de dados sequencial ou um membro PDS
- ffsput.log - O log do gravador de arquivos, que grava um conjunto de dados sequencial ou um membro PDS
- ffslock.log - O log do gerenciador de bloqueios, que bloqueia/desbloqueia um conjunto de dados sequencial ou um membro PDS
- rsecomm.log - O log do servidor RSE, que manipula os comandos do cliente e a criação de logs de comunicação de todos os serviços que dependem do RSE (pode conter rastreamento de pilha de exceção Java)

**Nota:**

- O diretório .eclipse e os arquivos de log .dstore\* começam com um ponto (.), o que os torna ocultos. Use o comando **ls -IA** do z/OS UNIX para listar arquivos e diretórios ocultos. Ao usar o cliente Developer for System z, selecione a página de preferências **Janela > Preferências... > Sistemas Remotos > Arquivos** e ative "Mostrar arquivos ocultos".
- daemon-home/server/  
Os arquivos de log específicos do daemon RSE e do conjunto de encadeamentos do RSE estão localizados em daemon-home/server, em que daemon-home é o valor da diretiva daemon.log em rsed.envvars. Se a diretiva daemon.log for comentada ou não estiver presente, o diretório inicial do ID do usuário designado à tarefa iniciada RSED será usado. O diretório inicial é definido no segmento de segurança OMVS do ID do usuário.
  - rsedaemon.log - O log do daemon RSE
  - rseserver.log - O log dos conjuntos de encadeamento RSE
  - audit.log - A trilha de auditoria do RSE
  - serverlogs.count - Contador para criação de log de fluxos do conjunto de encadeamento RSE
  - stderr.\*.log - Fluxo de erro padrão do conjunto de encadeamento RSE
  - stdout.\*.log - Fluxo de saída padrão do conjunto de encadeamento RSE
- /tmp  
Arquivos de log específicos de IVP (Installation Verification Program) estão localizados no diretório mencionado pelo TMPDIR, se esta variável for definida em rsed.envvars. Se a variável não for definida, os arquivos são criados no comando do operador /tmp.The **MODIFY LOGS** para a tarefa iniciada do RSED que também cria sua saída neste diretório.
  - fekfivpi.log - O log do teste IVP do fekfivpi
  - fekfivps.log - O log do teste IVP do fekfivps
  - fekfivpc.log - A criação de log de comunicação de teste do IVP, fekfivpc
  - feklogs.\* - Saída do comando do operador **MODIFY LOGS**

**Nota:** Há comandos do operador disponíveis para controlar a quantidade de dados gravados em alguns dos arquivos de log mencionados. Consulte "Comandos do operador" no *Guia de Configuração do Host* (SC23-7658) para obter informações adicionais.

## Criação de log do Debug Manager

- **SYSPRINT DD**

Criação de log de rastreo e criação de log de operações normais. O valor padrão na amostra JCL FEK.#CUST.PROCLIB(DBGMGR) é SYSOUT=\*.

## criação de logs do JES Job Monitor

- **SYSOUT DD**

Criação de logs de operações normais. O valor-padrão na amostra de JCL FEK.#CUST.PROCLIB(JMON) é SYSOUT=\*.

- **SYSPRINT DD**

Criação de logs de rastreo. O valor-padrão na amostra de JCL FEK.#CUST.PROCLIB(JMON) é SYSOUT=\*. O rastreo é ativado com o parâmetro -TV; consulte "rastreo do JES Job Monitor" na página 172 para obter detalhes adicionais.

## Criação de Log de Daemon RSE e de Conjunto de Encadeamento

- **STDOUT DD**

Os dados redirecionados de stdout, saída padrão Java de daemon RSE. O valor-padrão no JCL da amostra FEK.#CUST.PROCLIB(RSED) é SYSOUT=\*.

- **STDERR DD**

Os dados redirecionados de stderr, saída de erro padrão Java do daemon RSE. O valor-padrão no JCL da amostra FEK.#CUST.PROCLIB(RSED) é SYSOUT=\*.

- **daemon-home**

Os arquivos de log específicos do daemon RSE e do conjunto de encadeamentos do RSE estão localizados em daemon-home, em que daemon-home é o valor da diretiva daemon.log em rsed.envvars. Se a diretiva daemon.log for comentada ou não estiver presente, o diretório inicial do ID do usuário designado à tarefa iniciada RSED será usado. O diretório inicial é definido no segmento de segurança OMVS do ID do usuário.

- rsedaemon.log - O log do daemon RSE
- rseserver.log - O log dos conjuntos de encadeamento RSE
- audit.log - A trilha de auditoria do RSE
- serverlogs.count - Contador para criação de log de fluxos do conjunto de encadeamento RSE
- stderr.\*.log - Fluxo de erro padrão do conjunto de encadeamento RSE
- stdout.\*.log - Fluxo de saída padrão do conjunto de encadeamento RSE

**Nota:**

- serverlogs.count, stderr.\*.log e stdout.\*.log são criados apenas se a diretiva enable.standard.log em rsed.envvars estiver ativa ou se a função for dinamicamente ativada com o comando do operador **modify rsestandardlog on**.

- O \* em stderr\*.log e em stdout\*.log significa 1 por padrão. Entretanto, pode existir vários conjuntos de encadeamento RSE e, nesse caso, o número é aumentado para cada novo conjunto de encadeamento RSE para garantir nomes de arquivos exclusivos.
- Há comandos do operador disponíveis para controlar a quantidade de dados gravados em alguns dos arquivos de log mencionados. Consulte "Comandos do operador" no *Guia de Configuração do Host* (SC23-7658) para obter informações adicionais.
- Os arquivos rse\*.log também podem existir com uma extensão ".last", em vez de uma extensão ".log", se keep.last.log=true for especificado em rsed.envvars. Por padrão, os arquivos de log ".last" não são criados.
- Os arquivos rse\*.log terão um nome estendido se keep.all.logs=true for especificado em rsed.envvars. Por padrão, o nome estendido é usado. O nome a seguir é uma amostra do nome estendido, em que RSED representa o nome do espaço de endereço do daemon RSE e yyyymmddhhmmss é o registro de data e hora (ano, mês, dia, hora, minuto, segundo): rseserver.RSED#yyyymmddhhmmss.log

## criação de logs do usuário do RSE

- **userlog/\$LOGNAME/**

Há vários arquivos de log criados pelos componentes relacionados ao RSE. Todos estão localizados em userlog/\$LOGNAME/, em que userlog é o valor combinado das diretivas user.log e DSTORE\_LOG\_DIRECTORY em rsed.envvars, e \$LOGNAME é o ID do usuário de logon (em maiúsculas). Se a diretiva user.log for comentada ou não estiver presente, o caminho inicial do usuário será usado. O caminho inicial é definido no segmento de segurança OMVS do ID de usuário. Se a diretiva DSTORE\_LOG\_DIRECTORY for comentada ou não estiver presente, então .eclipse/RSE/ será anexado ao valor user.log.

- .dstoreMemLogging - Criação de log de uso de memória do armazenamento de dados
- .dstoreTrace - Criação de log de ação do armazenamento de dados
- .dstoreHashmap.\* - captura instantânea do hasmap do DataStore ativo
- .dstoreStackTrace.\* - captura instantânea dos encadeamentos do DataStore ativo e onde eles são chamados
- ffs.log - O log do servidor Foreign File System (FFS), que executa funções MVS nativas
- ffsget.log - O log do leitor de arquivos, que lê um conjunto de dados sequencial ou um membro PDS
- ffsput.log - O log do gravador de arquivos, que grava um conjunto de dados sequencial ou um membro PDS
- ffslock.log - O log do gerenciador de bloqueio que bloqueia ou desbloqueia um conjunto de dados sequencial ou um membro PDS
- rsecomm.log - O log do servidor RSE, que manipula os comandos do cliente e a criação de logs de comunicação de todos os serviços que dependem do RSE (pode conter rastreo de pilha de exceção Java)

### Nota:

- O diretório .eclipse e os arquivos de log .dstore\* começam com um ponto (.), o que os torna ocultos. Use o comando **ls -lA** do z/OS UNIX para listar arquivos e diretórios ocultos. Ao usar o cliente Developer for System z, selecione a página de preferências **Janela > Preferências... > Sistemas Remotos > Arquivos** e ative "Mostrar arquivos ocultos".

- A criação dos arquivos de log `.dstore*` é controlada pelas opções de inicialização `-DDSTORE_*` Java, conforme descrito em "Definindo parâmetros de inicialização Java com `_RSE_JAVAOPTS`" no *Guia de Configuração do Host* (SC23-7658).
- Os arquivos de log `.dstore*` são criados em UTF8. Use o comando z/OS UNIX `iconv -f UTF8 -t IBM-1047 .dstore*` para exibi-los no EBCDIC (ao usar página de código IBM-1047).
- Diferente dos arquivos `*.log`, os arquivos de log do `.dstore*` não são removidos automaticamente na reconexão do cliente. A remoção desses arquivos é uma ação manual.
- Há comandos do operador disponíveis para controlar a quantidade de dados gravados em alguns dos arquivos de log mencionados. Consulte "Comandos do operador" no *Guia de Configuração do Host* (SC23-7658) para obter informações adicionais.
- Os arquivos `ffs*.log` e `rsecomm.log` podem também existir com uma extensão `".last"` em vez de uma extensão `".log"` se `keep.last.log=true` estiver especificado em `rsed.envvars`. Por padrão, os arquivos de log `".last"` não são criados.
- Os arquivos de `ffs*.log` e `rsecomm.log` terão um nome estendido se `keep.all.logs=true` estiver especificado em `rsed.envvars`. Por padrão, o nome estendido é usado. O nome a seguir é uma amostra de nome estendido, em que `RSEDx` representa o nome do espaço de endereço do conjunto de encadeamentos no qual o usuário está ativo e `yyyymmddhhmmss` é um registro de data e hora (ano, mês, dia, hora, minuto, segundo): `ffs.RSEDx#yyyymmddhhmmss.log`

## criação de log do SCLM Developer Toolkit

- **userlog/\$LOGNAME/rsecomm.log**

A criação de log de comunicação do SCLM Developer Toolkit, em que `userlog` é o valor combinado das diretivas `user.log` e `DSTORE_LOG_DIRECTORY` em `rsed.envvars`, e `$LOGNAME` é o ID do usuário de logon (em maiúsculas). Se a diretiva `user.log` for comentada ou não estiver presente, o caminho inicial do usuário será usado. O caminho inicial é definido no segmento de segurança OMVS do ID de usuário. Se a diretiva `DSTORE_LOG_DIRECTORY` for comentada ou não estiver presente, então `.eclipse/RSE/` será anexado ao valor `user.log`.

## Criação de logs do CARMA

- **Tarefa do Servidor CARMA**

Ao abrir uma conexão com o CARMA e usar a interface em lote, `FEK.#CUST.SYSPROC(CRASUBMT)` iniciará uma tarefa do servidor (com o ID do usuário como proprietário) denominada `CRAport`, em que `port` é a porta TCP/IP usada.

- **CARMALOG DD**

Se a instrução DD `CARMALOG` for especificada no método de inicialização do CARMA escolhido, a criação de logs do CARMA será redirecionada para essa instrução DD na tarefa do servidor, caso contrário, ela irá para `SYSPRINT`.

- **SYSPRINT DD**

O `SYSPRINT DD` da tarefa do servidor conterà a criação de log do CARMA, se o `CARMALOG` da instrução DD não estiver definido.

- **SYSTSPRT DD**

O `SYSTSPRT DD` da tarefa do servidor mantém as mensagens do sistema (TSO) da inicialização do servidor CARMA.

- **userlog/\$LOGNAME/rsecomm.log**

A criação de log de comunicação de CARMA, em que userlog é o valor combinado das diretivas user.log e DSTORE\_LOG\_DIRECTORY em rsed.envvars, e \$LOGNAME é o DI do usuário de logon (em maiúsculas). Se a diretiva user.log for comentada ou não estiver presente, o caminho inicial do usuário será usado. O caminho inicial é definido no segmento de segurança OMVS do ID de usuário. Se a diretiva DSTORE\_LOG\_DIRECTORY for comentada ou não estiver presente, então .eclipse/RSE/ será anexado ao valor user.log.

## **Criação de Log IVP fekfivpc**

- **/tmp/fekfivpc.log**

O comando fekfivpc (teste do IVP relacionado ao CARMA) criará o arquivo fekfivpc.log para documentar a comunicação entre o RSE e o CARMA. O log será criado no diretório conhecido por TMPDIR, se esta variável for definida no rsed.envvars. Se a variável não for definida, o arquivo será criado no /tmp.

## **Criação de log de teste IVP do fekfivpi**

- **/tmp/fekfivpi.log**

Saída do comando fekfivpi -file (teste do IVP relacionado ao TSO/ISPF Client Gateway). O log será criado no diretório conhecido por TMPDIR, se esta variável for definida no rsed.envvars. Se a variável não for definida, o arquivo será criado no /tmp.

## **Criação de Log de Teste IVP do fekfivps**

- **/tmp/fekfivps.log**

Saída do comando fekfivps -file (teste do IVP relacionado ao SCLMDT). O log será criado no diretório conhecido por TMPDIR, se esta variável for definida no rsed.envvars. Se a variável não for definida, o arquivo será criado no /tmp.

## **Criação de Log da Revisão de Código**

- **SYSTSPRT DD**

O SYSTSPRT DD da etapa que chama o procedimento de revisão de código retém as mensagens do frontend que conduz o processo de análise de código.

- **WORKSPCE DD**

O WORKSPCE DD da etapa que chama o procedimento de revisão de código retém as mensagens de log da área de trabalho do Eclipse do processo de análise de código.

- **ERRMSGs DD**

O ERRMSGs DD da etapa que chama o procedimento de revisão de código retém a saída stderr do processo de análise de código.

## **Criação de Log da Cobertura de Código**

- **SYSTSPRT DD**

O SYSTSPRT DD da etapa que chama o procedimento de revisão de código retém as mensagens do front-end que conduz o processo de análise de código.

- **WORKSPCE DD**

O WORKSPCE DD da etapa que chama o procedimento de revisão de código retém as mensagens de log da área de trabalho do Eclipse do processo de análise de código.

- **ERRMSGs DD**



O ERRMSG DD da etapa que chama o procedimento de revisão de código retém a saída stderr do processo de análise de código.

---

## Arquivos de dump

Quando um produto é finalizado de forma anormal, um dump de armazenamento é criado para auxiliar na determinação do problema. A disponibilidade e o local desses dumps dependem quase que totalmente das configurações específicas do site. Os dumps podem não ser criados, ou podem ser criados em locais diferentes daqueles mencionados nas seções a seguir.

### Dumps do MVS

Quando um programa está em execução no MVS, verifique os arquivos de dump do sistema e verifique a JCL em busca das seguintes instruções DD (dependendo do produto):

- SYSABEND
- SYSMDUMP
- SYSUDUMP
- CEEDUMP
- SYSPRINT
- SYSOUT

Consulte o *MVS JCL Reference* (SA22-7597) e o *Language Environment Debugging Guide* (GA22-7560) para obter informações adicionais sobre essas instruções DD.

### Dumps de Java

No z/OS UNIX, a maioria dos dumps do Developer for System z é controlada pela Java Virtual Machine (JVM).

A JVM cria um conjunto de agentes de dump por padrão, durante a inicialização (SYSTDUMP e JAVADUMP). Você pode sobrepor este conjunto de agentes de dump utilizando a variável de ambiente JAVA\_DUMP\_OPTS e sobrepor o conjunto pelo uso de -Xdump na linha de comandos. As opções da linha de comandos JVM são definidas na diretiva \_RSE\_JAVA\_OPTS de rsed.envvars. Não altere nenhuma configuração de dump, a menos que tenha sido solicitado pelo IBM Support Center.

**Nota:** A opção -Xdump:what na linha de comandos pode ser usada para determinar quais agentes de dump existem na conclusão da inicialização.

Os tipos de dump que podem ser produzidos são os seguintes:

#### SYSTDUMP

Dump de transação Java. Um dump de armazenamento não formatado gerado pelo z/OS.

O dump é gravado em um conjunto de dados MVS sequencial utilizando-se um nome padrão no formato %uid.JVM.TDUMP.%job.D%y%m%d.T%H%M%S, ou conforme determinado pela configuração da variável de ambiente JAVA\_DUMP\_TDUMP\_PATTERN.

**Nota:** JAVA\_DUMP\_TDUMP\_PATTERN permite o uso de variáveis, que são convertidas em um valor real na hora em que o dump de transação é obtido.



**Tabela 43. Variáveis de JAVA\_DUMP\_TDUMP\_PATTERN**

| Variável | Uso                 |
|----------|---------------------|
| %uid     | ID do usuário       |
| %job     | Nome da tarefa      |
| %y       | Ano (2 dígitos)     |
| %m       | Mês (2 dígitos)     |
| %d       | Dia (2 dígitos)     |
| %H       | Hora (2 dígitos)    |
| %M       | Minuto (2 dígitos)  |
| %S       | Segundo (2 dígitos) |

### CEEDUMP

Dump do LE (Language Environment). Um dump do sistema de resumo formatado que mostra rastreios de pilha para cada encadeamento que está no processo JVM, junto com informações de registro e um dump curto de armazenamento para cada registro.

O dump é gravado em um arquivo z/OS UNIX chamado CEEDUMP.aaaammdd.hhmmss.pid, em que aaaammdd é igual à data atual, hhmmss é a hora atual e pid é o ID do processo atual. Os locais possíveis deste arquivo são descritos em "Locais de Dump do z/OS UNIX".

### HEAPDUMP

Um dump formatado (uma lista) dos objetos que estão no heap Java.

O dump é gravado em um arquivo z/OS UNIX chamado HEAPDUMP.aaaammdd.hhmmss.pid.TXT, em que aaaammdd é igual à data atual, hhmmss é a hora atual e pid é o ID do processo atual. Os locais possíveis deste arquivo são descritos em "Locais de Dump do z/OS UNIX".

Note que o Developer for System z fornece um comando do operador para acionar este dump. Consulte o capítulo "Comandos do Operador" no *Guia de Configurações do Host* (SC23-7658) para obter mais detalhes.

### JAVADUMP

Uma análise formatada da JVM. Contém informações de diagnóstico relacionadas à JVM e ao aplicativo Java, como o ambiente de aplicativos, encadeamentos, pilha nativa, bloqueios e memória.

O dump é gravado em um arquivo z/OS UNIX chamado JAVADUMP.aaaammdd.hhmmss.pid.TXT, em que aaaammdd é igual à data atual, hhmmss é a hora atual e pid é o ID do processo atual. Os locais possíveis deste arquivo são descritos em "Locais de Dump do z/OS UNIX".

Note que o Developer for System z fornece um comando do operador para acionar este dump. Consulte o capítulo "Comandos do Operador" no *Guia de Configurações do Host* (SC23-7658) para obter mais detalhes.

Consulte o *Java Diagnostic Guide* (SC34-6358) para obter informações adicionais sobre dumps de JVM e o *Language Environment Debugging Guide* (GA22-7560) para obter informações específicas de LE.

## Locais de Dump do z/OS UNIX

A JVM verifica a existência de cada um dos seguintes locais e as permissões de gravação e armazena os arquivos CEEDUMP, HEAPDUMP e JAVADUMP no primeiro local disponível. Observe que você deve possuir espaço em disco livre suficiente para que o arquivo de dump seja gravado corretamente.

1. O diretório na variável de ambiente `_CEE_DMPTARG`, se localizado. Essa variável está configurada em `rsed.envvars` como `/tmp`. Ela pode ser alterada para `/dev/null` para evitar a criação de arquivos dump.
2. O diretório de trabalho atual, se o diretório não for o diretório raiz (`/`) e se o diretório for gravável.
3. O diretório na variável de ambiente `TMPDIR` (uma variável de ambiente que indica o local de um diretório temporário se ele não for `/tmp`), se localizado.
4. O diretório `/tmp`.
5. Se o dump não puder ser armazenado em nenhum dos locais mencionados anteriormente, ele será colocado em `stderr`.

---

## Rastreio

### Rastreio do Debug Manager

O rastreio do Debug Manager é controlado pelo operador do sistema, conforme descrito em "Comandos do operador" no *Guia de Configuração do Host* (SC23-7658).

- Iniciar a tarefa iniciada do DBGMR com o parâmetro `PRM=DEBUG` ativa o rastreio.
- O comando do operador **modify loglevel** permite selecionar o nível de detalhe desejado para mensagens de log.

### rastreio do JES Job Monitor

O rastreio do JES Job Monitor é controlado pelo operador do sistema, conforme descrito em "Comandos do operador" no *Guia de Configuração do Host* (SC23-7658).

- Inicializar a tarefa iniciada JMON com o parâmetro `PRM=-TV` ativa o modo detalhado (rastreio)
- Os comandos do operador **modify trace** e **modify message** permitem selecionar o nível de detalhe desejado das mensagens de log.

### rastreio RSE

Há vários arquivos de log criados pelos componentes relacionados ao RSE. A maioria está localizada em `userlog/$LOGNAME/`, em que `userlog` é o valor combinado das diretivas `user.log` e `DSTORE_LOG_DIRECTORY` em `rsed.envvars`, e `$LOGNAME` é o ID do usuário de logon (em maiúsculas). Se a diretiva `user.log` for comentada ou não estiver presente, o caminho inicial do usuário será usado. O caminho inicial é definido no segmento de segurança OMVS do ID de usuário. Se a diretiva `DSTORE_LOG_DIRECTORY` for comentada ou não estiver presente, então `.eclipse/RSE/` será anexado ao valor `user.log`.

A quantidade de dados gravados em `ffs*.log` e `rsecomm.log` é controlada pelo comando do operador **modify rsecommlog** ou pela configuração de `debug_level` in `rsecomm.properties`. Consulte "Comandos do operador" no *Guia de Configuração do Host* (SC23-7658) e "(Opcional) Rastreio RSE" no *Guia de Configuração do Host* (SC23-7658) para obter detalhes adicionais.

A criação dos arquivos de log `.dstore*` é controlada pelas opções de inicialização `-DDSTORE_* Java`, conforme descrito em "Definindo parâmetros de inicialização Java com `_RSE_JAVAOPTS`" no *Guia de Configuração do Host* (SC23-7658).

#### Nota:

- O diretório `.eclipse` e os arquivos de log `.dstore*` começam com um ponto (`.`), o que os torna ocultos. Use o comando `ls -lA` do z/OS UNIX para listar

arquivos e diretórios ocultos. Ao usar o cliente Developer for System z, selecione a página de preferências **Janela > Preferências... > Sistemas Remotos > Arquivos** e ative “Mostrar arquivos ocultos”.

- Os arquivos de log `.dstore*` são criados em UTF8. Use o comando `z/OS UNIX iconv -f UTF8IBM-1047 .dstore*` para exibi-los no EBCDIC (ao usar a página de códigos IBM-1047).
- Diferente dos arquivos `*.log`, os arquivos de log do `.dstore*` não são removidos automaticamente na reconexão do cliente. A remoção desses arquivos é uma ação manual.

Os arquivos de log específicos do daemon RSE e do conjunto de encadeamentos do RSE estão localizados em `daemon-home`, em que `daemon-home` é o valor da diretiva `daemon.log` em `rsed.envvars`. Se a diretiva `daemon.log` for comentada ou não estiver presente, o diretório inicial do ID do usuário designado à tarefa iniciada RSED será usado. O diretório inicial é definido no segmento de segurança OMVS do ID do usuário.

A quantidade de dados gravada em `rsedaemon.log` e em `rserver.log` é controlada pelos comandos do operador **modify rsedaemonlog** e **modify rserverlog** ou configurando `debug_level` em `rsecomm.properties`. Consulte "Comandos do operador" no *Guia de Configuração do Host* (SC23-7658) e "(Opcional) Rastreo RSE" no *Guia de Configuração do Host* (SC23-7658) para obter detalhes adicionais.

`serverlogs.count`, `stderr*.log` e `stdout*.log` são criados apenas se a diretiva `enable.standard.log` em `rsed.envvars` estiver ativa, ou se a função for dinamicamente ativada com o comando do operador **modify rsestandardlog on**.

## rastreio CARMA

O usuário pode controlar a quantidade de informações de rastreio que um servidor CARMA gera ao configurar o Nível de Rastreio na guia de Propriedades na conexão CARMA no cliente. As opções para o Nível de Rastreio são:

- Desativar Criação de Log
- Log de Erros
- Log de Avisos
- Log Informativo
- Log de Depuração

O valor-padrão é o seguinte:

Log de Erros

Consulte “Arquivos de Log” na página 164 para obter informações adicionais sobre as localizações do arquivo de log.

O programador do sistema z/OS pode controlar a quantidade de informações de rastreio que o método de inicialização do CARMA's CRASTART gera, configurando `crastart.syslog` em `CRASRV.properties`, e configurando o nível de depuração para `rsecomm.log` em `rsecomm.properties` ou com um comando do operador.

## Rastreio de feedback de erro

O procedimento a seguir permite reunir informações necessárias para diagnosticar problemas de feedback de erro com procedimentos de construção remota. Esse

rastreio causará diminuição no desempenho e deverá ser realizado somente sob a orientação do IBM Support Center. Todas as referências a hlq neste seção referem-se ao qualificador de alto nível usado durante a instalação do Developer for System z. O padrão da instalação é FEK, mas isto talvez não se aplique ao seu site.

1. Faça uma cópia de backup do procedimento de compilação ELAXFC0C ativo. Este procedimento é enviado por padrão no conjunto de dados hlq.SFEKSAMP, mas pode ter sido copiado para um local diferente (por exemplo, SYS1.PROCLIB), conforme descrito em "Procedimentos de construção remota ELAXF\*" no *Guia de Configuração do Host* (SC23-7658).
2. Altere o procedimento ELAXFC0C ativo para incluir a cadeia 'MAXTRACE' na opção de compilação EXIT(ADEXIT(ELAXMGUX)).

```
//COBOL EXEC PGM=IGYCRCTL,REGION=2048K,
//* PARM=('EXIT(ADEXIT(ELAXMGUX))'),
// PARM=('EXIT(ADEXIT(''MAXTRACE'',ELAXMGUX))'),
// 'ADATA',
// 'LIB',
// 'TEST(NONE,SYM,SEP)',
// 'LIST',
// 'FLAG(I,I)'&CICS &DB2 &COMP)
```

**Nota:** É necessário duplicar os apóstrofes em MAXTRACE. A opção agora é: EXIT(ADEXIT(''MAXTRACE'',ELAXMGUX)).

3. Execute uma Verificação de Sintaxe Remota no programa COBOL para o qual você deseja rastreio detalhado.
4. A parte SYSOUT da saída JES começará listando os nomes dos conjuntos de dados para SIDEFILE1, SIDEFILE2, SIDEFILE3 e SIDEFILE4.

```
ABOUT TOO OPEN SIDEFILE1 - NAME = 'uid.DT021207.TT110823.M0000045.C0000000'
SUCCESSFUL OPEN SIDEFILE1 - NAME = 'uid.DT021207.TT110823.M0000045.C0000000'
ABOUT TOO OPEN SIDEFILE2 - NAME = 'uid.DT021207.TT110823.M0000111.C0000001'
SUCCESSFUL OPEN SIDEFILE2 - NAME = 'uid.DT021207.TT110823.M0000111.C0000001'
ABOUT TOO OPEN SIDEFILE3 - NAME = 'uid.DT021207.TT110823.M0000174.C0000002'
SUCCESSFUL OPEN SIDEFILE3 - NAME = 'uid.DT021207.TT110823.M0000174.C0000002'
ABOUT TOO OPEN SIDEFILE4 - NAME = 'uid.DT021207.TT110823.M0000236.C0000003'
SUCCESSFUL OPEN SIDEFILE4 - NAME = 'uid.DT021207.TT110823.M0000236.C0000003'
```

**Nota:** Dependendo das suas configurações, SIDEFILE1 e SIDEFILE2 podem estar apontando para uma instrução DD (SUCCESSFUL OPEN SIDEFILE1 - NAME = DD:WSEDSF1). Consulte a parte JESJCL da saída (localizada antes da parte SYSOUT) para obter o nome real do conjunto de dados.

```
22 //COBOL.WSEDSF1 DD DISP=MOD,
// DSN=uid.ERRCOB.member.SF.Z682746.XML
23 //COBOL.WSEDSF2 DD DISP=MOD,
// DSN=uid.ERRCOB.member.SF.Z682747.XML
```

5. Copie esses quatro conjuntos de dados em seu PC, por exemplo, criando um projeto COBOL local no Developer for System z e incluindo os conjuntos de dados SIDEFILE1->4.
6. Copie o log da tarefa do JES completo em seu PC, por exemplo, abrindo a saída de tarefas no Developer for System z e salvando-a no projeto local selecionando **Arquivo > Salvar Como ....**
7. Restaure o procedimento ELAXFC0C para o estado original, desfazendo a alteração (remova a cadeia "MAXTRACE" nas opções de compilação) ou restaurando o backup.
8. Envie os arquivos coletados (SIDEFILE1->4 e log da tarefa) para o centro de suporte IBM.

---

## Bits de permissão do z/OS UNIX

O Developer for System z requer que o sistema de arquivo z/OS UNIX e alguns arquivos z/OS UNIX tenham certos bits de permissão configurados.

## atributo do sistema de arquivos SETUID

O Explorador de Sistema Remoto (RSE) é o componente do Developer for System z que fornece serviços principais, como conectar o cliente ao host. Ele deve ter permissão para executar tarefas como criar o ambiente de segurança do usuário.

O sistema de arquivos (HFS ou zFS) em que o Developer for System z está instalado deve ser montado com o bit de permissão SETUID ativado (este é o padrão do sistema). A montagem do sistema de arquivo com o parâmetro NOSETUID impedirá o Developer for System z de criar o ambiente de segurança do usuário e falhará no pedido de conexão. Outros indicadores para este problema de configuração são:

- mensagem do console "FEK999E: O módulo fekfomvs deve ser marcado como autorizado pelo APF"
- O PassTicket IVP falha com "ICH409I 282-010 FOI ENCERRADO DE FORMA ANORMAL DURANTE O PROCESSAMENTO DE RACHECK"

Erros semelhantes (tais como as mensagens BPXP014I e BPXP015I) podem ser esperados se os sistemas de arquivos que hospedam binários de Java ou z/OS UNIX são montados com o parâmetro NOSETUID.

Use o comando TSO **ISHELL** para listar o status atual do bit SETUID. No painel ISHELL, selecione **Sistemas\_de\_arquivos > 1. Montar tabela...** para listar os sistemas de arquivos montados. O comando da linha **a** mostrará os atributos para o sistema de arquivos selecionado, em que o campo "Ignorar SETUID" deve ser 0.

## Autorização de controle de programa

O Explorador de Sistema Remoto (RSE) é o componente do Developer for System z que fornece serviços principais, como conectar o cliente ao host. Ele deve executar o programa controlado para realizar tarefas como a comutação para o ID do usuário do cliente.

O bit de controle de programa do z/OS UNIX é configurado durante a instalação do SMP/E onde necessário, exceto para a interface Java para seu produto de segurança, conforme documentado no Capítulo 2, "Considerações de segurança", na página 19. Este bit de permissão pode se perder caso você não o tenha preservado durante uma cópia manual dos diretórios Developer for System z.

Os seguintes arquivos do Developer for System z devem ser controlados pelo programa:

- /usr/lpp/rdz/bin/
  - fekfdivp
  - fekfomvs
  - fekfrivp
- /usr/lpp/rdz/lib/
  - fekfdir.dll
  - libfekdcore.so
  - libfekfmain.so
- /usr/lpp/rdz/lib/icuc/
  - libicudata.dll
  - libicudata50.1.dll
  - libicudata50.dll

```

- libicudata64.50.1.dll
- libicudata64.50.dll
- libicudata64.dll
- libicuuc.dll
- libicuuc50.1.dll
- libicuuc50.dll
- libicuuc64.50.1.dll
- libicuuc64.50.dll
- libicuuc64.dll

```

Use o comando do z/OS UNIX, **ls -E**, para listar os atributos estendidos, em que o bit de controle de programa é marcado com a letra p, conforme exibido na amostra a seguir (\$ é o prompt do z/OS UNIX):

```

$ cd /usr/lpp/rdz
$ ls -E lib/fekf*
-rwxr-xr-x -ps- 2 user group 94208 Jul 8 12:31 lib/fekfdir.dll

```

Use o comando **extattr +p** do z/OS UNIX para configurar o bit de controle de programa manualmente, conforme exibido na seguinte amostra (\$ e # são o prompt do z/OS UNIX):

```

$ cd /usr/lpp/rdz
$ su
extattr +p lib/fekf*
exit
$ ls -E lib/fekf*
-rwxr-xr-x -ps- 2 user group 94208 Jul 8 12:31 lib/fekfdir.dll

```

**Nota:** Para utilizar o comando **extattr +p**, você deve ter pelo menos acesso de LEITURA ao perfil BPX.FILEATTR.PROGCTL na classe FACILITY do software de segurança ou ser um superusuário (UID 0) se esse perfil não estiver definido. para obter informações adicionais, consulte *UNIX System Services Planning* (GA22-7800).

## Autorização APF

O Explorador de Sistema Remoto (RSE) é o componente do Developer for System z que fornece serviços principais, como conectar o cliente ao host. Ele deve executar autorizado pelo APF a fim de executar tarefas como exibir uso de recurso de processo detalhado.

O bit APF z/OS UNIX é definido durante a instalação do SMP/E onde necessário. Este bit de permissão pode se perder caso você não o tenha preservado durante uma cópia manual dos diretórios Developer for System z.

Os arquivos do Developer for System z a seguir devem ser autorizados pelo APF:

- /usr/lpp/rdz/bin/
  - CRASTART
  - fekfomvs
  - fekfriwp

Use o comando do z/OS UNIX, **ls -E**, para listar os atributos estendidos, em que o bit APF é marcado com a letra a, conforme exibido na amostra a seguir (\$ é o prompt do z/OS UNIX):

```

$ cd /usr/lpp/rdz
$ ls -E bin/fekfriwp
-rwxr-xr-x -aps- 2 user group 114688 Sep 17 06:41 bin/fekfriwp

```

Use o comando **extattr +a** do z/OS UNIX para configurar o bit APF manualmente, conforme exibido na amostra a seguir (\$ e # são os prompts do z/OS UNIX):

```
$ cd /usr/lpp/rdz
$ su
extattr +a bin/fekfrivp
exit
$ ls -l bin/fekfrivp
-rwxr-xr-x 2 user group 114688 Sep 17 06:41 bin/fekfrivp
```

**Nota:** Para que seja possível usar o comando **extattr +a**, você deve ter ao menos o acesso de LEITURA no perfil BPX.FILEATTR.APF na classe FACILITY do seu software de segurança ou ser um superusuário (UID 0), caso este perfil não esteja definido. para obter informações adicionais, consulte *UNIX System Services Planning* (GA22-7800).

## Sticky Bit

Alguns dos serviços opcionais do Developer for System z requerem que os módulos de carregamento do MVS estejam disponíveis para o z/OS UNIX. Isso é feito ao criar um stub (um arquivo fictício) no z/OS UNIX com o bit "sticky" ativado. Quando o stub é executado, o z/OS UNIX procurará um módulo de carregamento MVS com o mesmo nome e executará o módulo de carregamento em vez disso.

O sticky bit do z/OS UNIX é configurado durante a instalação do SMP/E onde necessário. Esses bits de permissão podem ser perdidos se você não os preservou durante uma cópia manual dos diretórios do Developer for System z.

Os arquivos do Developer for System z a seguir devem ter o sticky bit em:

- /usr/lpp/rdz/bin/
  - AZUTSTRN
  - CRASTART

Use o comando **ls -l** do z/OS UNIX para listar as permissões, em que o sticky bit é marcado com a letra **t**, conforme exibido na seguinte amostra (\$ é o prompt do z/OS UNIX):

```
$ cd /usr/lpp/rdz
$ ls -l bin/CRA*
-rwxr-xr-t 2 user group 71 Jul 8 12:31 bin/CRASTART
```

Utilize o comando **chmod +p** do z/OS UNIX para configurar o sticky bit manualmente, conforme exibido na seguinte amostra (\$ e # é o prompt do z/OS UNIX):

```
$ cd /usr/lpp/rdz
$ su
chmod +t bin/CRA*
exit
$ ls -l bin/CRA*
-rwxr-xr-t 2 user group 71 Jul 8 12:31 bin/CRASTART
```

**Nota:** Para poder utilizar o comando **chmod**, você deve ter pelo menos o acesso READ ao perfil SUPERUSER.FILESYS.CHANGEPERMS na classe UNIXPRIV do software de segurança ou ser um superusuário (UID 0) se esse perfil não estiver definido. para obter informações adicionais, consulte *UNIX System Services Planning* (GA22-7800).

---

## Portas TCP/IP reservadas

Com o comando **netstat** (TSO ou z/OS UNIX), você pode obter uma visão geral das portas atualmente em uso. A saída desse comando será semelhante ao exemplo a seguir. As portas usadas são o último número (atrás de "...") na coluna "Soquete Local". Como estas portas já estão em uso, elas não podem ser usadas para a configuração do Developer for System z.

IPv4



```

MVS TCP/IP NETSTAT CS VxRy TCPIP Name: TCPIP 16:36:42
User Id Conn Local Socket Foreign Socket State

BPX0INIT 00000014 0.0.0.0..10007 0.0.0.0..0 Listen
INETD4 00000040 0.0.0.0..512 0.0.0.0..0 Listen
RSED 0000004B 0.0.0.0..4035 0.0.0.0..0 Listen
JMON 00000038 0.0.0.0..6715 0.0.0.0..0 Listen

```

## IPv6

```

MVS TCP/IP NETSTAT CS VxRy TCPIP Name: TCPIP 12:46:25
User Id Conn State

BPX0INIT 00000018 Listen
Local Socket: 0.0.0.0..10007
Foreign Socket: 0.0.0.0..0
INETD4 00000046 Listen
Local Socket: 0.0.0.0..512
Foreign Socket: 0.0.0.0..0
RSED 0000004B Listen
Local Socket: 0.0.0.0..4035
Foreign Socket: 0.0.0.0..0
JMON 00000037 Listen
Local Socket: 0.0.0.0..6715
Foreign Socket: 0.0.0.0..0

```

Outra limitação que pode existir são as portas TCP/IP reservadas. Há os dois lugares comuns a seguir para reservar as portas TCP/IP:

### • PROFILE.TCPIP

Esse é o conjunto de dados referido pela instrução PROFILE DD da tarefa iniciada do TCP/IP, muitas vezes chamado de SYS1.TCPPARMS(TCPPROF).

- PORT: Reserva uma porta para nomes de tarefas especificados.
- PORTRANGE: Reserva um intervalo de portas para nomes de tarefas especificados.

Consulte o *Servidor de Comunicações: Guia de Configuração do IP* (SC31-8775) para obter mais informações sobre estas instruções.

### • SYS1.PARMLIB(BPXPRMxx)

- INADDRANYPORT: Especifica o número da porta inicial para o intervalo de números de portas que o sistema reserva para utilização com PORT 0, ligações INADDR\_ANY. Esse valor é necessário somente para CINET (várias pilhas TCP/IP ativas em um único host).
- INADDRANYCOUNT: Especifica o número de portas que o sistema reserva, iniciando com o número de porta especificado no parâmetro INADDRANYPORT. Esse valor é necessário somente para CINET (várias pilhas TCP/IP ativas em um único host).

Consulte *UNIX Planejamento de Serviços do Sistema* (GA22-7800) e *MVS Referência de Inicialização e Ajuste* (SA22-7592) para obter mais informações sobre estas instruções.

Estas portas reservadas podem ser listadas com o comando **netstat portl** (TSO ou z/OS UNIX), que cria uma saída como esta do exemplo a seguir:

```

MVS TCP/IP NETSTAT CS VxRy TCPIP Name: TCPIP 17:08:32
Port# Prot User Flags Range IP Address

00007 TCP MISC SERV DA
00009 TCP MISC SERV DA
00019 TCP MISC SERV DA
00020 TCP OMVS D
00021 TCP FTPD1 DA
00025 TCP SMTP DA
00053 TCP NAMESRV DA
00080 TCP OMVS DA
03500 TCP OMVS DAR 03500-03519
03501 TCP OMVS DAR 03500-03519

```

Consulte *Communications Server: IP System Administrator's Commands* (SC31-8781) para obter informações adicionais sobre o comando **NETSTAT**.

**Nota:** O comando **NETSTAT** mostra somente as informações definidas em **PROFILE.TCPIP**, que devem sobrepor as definições de **BPXPRMxx**. Em caso de dúvidas ou problemas, verifique o membro **parmlib** de **BPXPRMxx** para verificar as portas sendo reservadas aqui.

---

## Tamanho do espaço de endereço

O daemon **RSE**, que é um processo **z/OS UNIX Java**, exige um tamanho de região grande para executar suas funções. Portanto, é importante definir limites de armazenamento grandes para espaços de endereço do **OMVS**.

## Requisitos da JCL de Inicialização

O daemon **RSE** é iniciado pela **JCL** utilizando **BPXBATSL**, cujo tamanho da região deve ser 0.

## Limitações Definidas em SYS1.PARMLIB(BPXPRMxx)

Configure **MAXASSIZE** em **SYS1.PARMLIB(BPXPRMxx)**, que define o tamanho da região do espaço de endereço (processo) do **OMVS** como 2G. Esse é o tamanho máximo permitido. Esse é um limite amplo do sistema e, dessa forma, ativo em todos os espaços de endereço do **z/OS UNIX**. Se não for desejado, será possível configurar o limite também apenas para o **Developer for System z** em seu software de segurança.

Esse valor pode ser verificado e configurado dinamicamente (até o próximo **IPL**) com os seguintes comandos de console, conforme descrito em *MVS System Commands* (GC28-1781):

1. **DISPLAY OMVS,0**
2. **SETOMVS MAXASSIZE=2G**

## Limitações Armazenadas no Perfil de Segurança

Verifique **ASSIZEMAX** no segmento **OMVS** do **ID** do usuário do daemon e configure-o como 2147483647 ou, de preferência, como **NONE** para utilizar o valor **SYS1.PARMLIB(BPXPRMxx)**.

Utilizando **RACF**, esse valor pode ser verificado e configurado com os seguintes comandos **TSO**, conforme descrito em *Security Server RACF Command Language Reference* (SA22-7687):

1. **LISTUSER userid NORACF OMVS**
2. **ALTUSER userid OMVS(NOASSIZEMAX)**

## Limitações Impostas por Saídas do Sistema

Certifique-se de não permitir que saídas do sistema **IEFUSI** ou **IEALIMIT** controlem os tamanhos de regiões de espaços de endereços **OMVS**. Uma forma possível de fazer isso é pela codificação de **SUBSYS(OMVS,NOEXITS)** em **SYS1.PARMLIB(SMFPRMxx)**.

Os valores **SYS1.PARMLIB(SMFPRMxx)** podem ser verificados e ativados com os seguintes comandos do console, conforme descrito em *MVS System Commands* (GC28-1781):

1. **DISPLAY SMF,0**
2. **SET SMF=xx**

## Limitações para Endereçamento de 64 Bits

A palavra-chave **MEMLIMIT** em **SYS1.PARMLIB(SMFPRMxx)** limita o quanto uma tarefa de armazenamento virtual de 64 bits pode alocar acima da barra de 2GB. Ao contrário do parâmetro **REGION** no JCL, o **MEMLIMIT=0M** significa que o processo não pode usar o armazenamento virtual acima da barra.

Se o **MEMLIMIT** não estiver especificado em **SMFPRMxx**, o valor-padrão será **0M**, assim as tarefas serão limitadas ao (31 bits) 2GB abaixo da barra. O padrão alterado no z/OS 1.10 para 2G, permitindo que as tarefas de 64 bits usem até 4GB (os 2GB abaixo da barra e os 2GB acima da barra concedidos por **MEMLIMIT**).

Os valores **SYS1.PARMLIB(SMFPRMxx)** podem ser verificados e ativados com os seguintes comandos do console, conforme descrito em *MVS System Commands* (GC28-1781):

1. **DISPLAY SMF,0**
2. **SET SMF=xx**

O **MEMLIMIT** também pode ser especificado como parâmetro na placa **EXEC** no JCL. Se nenhum parâmetro **MEMLIMIT** estiver especificado, o padrão será o valor definido para **SMF**, exceto quando o **REGION=0M** estiver especificado, em tal caso o padrão será **NOLIMIT**.

---

## Informações Variadas

### Encerramento Anormal por Falta de Espaço B37 de Feedback de Erro

Quando um usuário seleciona o feedback de erro durante uma ação de compilação, vários conjuntos de dados temporários são criados pelo Developer for System z. Quando um desses conjuntos de dados tem falta de espaço, as tarefas de compilação terminam com um encerramento anormal por falta de espaço B37-04.

Ajuste a alocação de espaço em **FEK.SFEKPROC(FEKFERRF)** quando os usuários tiverem esse problema. O valor padrão é **SPACE(200,40) TRACKS**.

### Limites do sistema

**SYS1.PARMLIB(BPXPRMxx)** define muitas limitações relacionadas ao z/OS UNIX, que pode ser acessado quando muitos clientes do Developer for System z estão ativos. A maioria dos valores de **BPXPRMxx** pode ser alterada dinamicamente com os comandos do console **SETOMVS** e **SET OMVS**.

Use o comando do console **SETOMVS LIMMSG=ALL** para que o z/OS UNIX exiba mensagens do console (BPXI040I) quando qualquer dos limites **BPXPRMxx** estiver prestes a ser atingido.

### Conexão recusada

Cada conexão RSE inicia diversos processos que são permanentemente ativos. Novas conexões podem ser recusadas devido ao limite configurado em **SYS1.PARMLIB(BPXPRMxx)** na quantidade de processos, especialmente quando os usuários compartilham o mesmo UID (como ao utilizar o segmento **OMVS** padrão).

- O limite por UID é definido pela palavra-chave **MAXPROCUSER** e possui um valor-padrão de 25.

- O limite do sistema é definido pela palavra-chave MAXPROCSYS e possui um valor-padrão de 200.

Outra origem de conexões recusadas é o limite da quantidade de espaços de endereço do z/OS e de usuários do z/OS UNIX ativos.

- A quantidade máxima de Address Space IDs (ASID) é definida em SYS1.PARMLIB(IEASYSxx) com a palavra-chave MAXUSER e tem valor-padrão de 255.
- A quantidade máxima de UIDs (z/OS UNIX User IDs) é definida em SYS1.PARMLIB(BPXPRMxx) com a palavra-chave MAXUIDS e possui o valor-padrão de 200.

## OutOfMemoryError

Um conjunto de encadeamentos do RSE pode falhar com uma mensagem OutOfMemoryError sendo registrada. Esse erro está relacionado ao tamanho do heap Java e pode ocorrer se os usuários ativos deste conjunto de encadeamentos usarem mais recursos do que o esperado. As causas comuns desse erro são as seguintes:

- Expandindo filtros de grandes conjuntos de dados no Explorador de Sistema Remoto
- Abrindo PDS(E) com uma grande quantidade de membros
- Abrindo grandes arquivos de membros ou sequenciais

Para resolver esse problema, é possível fazer o seguinte:

- Aumentar a diretiva -Xmx em rsed.envvars, porque ela controla o tamanho máximo do heap Java. Observe que o heap Java deve se ajustar dentro dos limites de espaço de endereço.
- Diminuir a diretiva -Dmaximum.clients em rsed.envvars, porque ela controla quantos usuários podem ser colocados em um único conjunto de encadeamento (e também compartilhar um único heap Java).

---

## Emulador de Conexão do Host

- O Emulador de Conexão do Host utiliza o telnet TN3270, e não o servidor RSE, para se conectar ao host.
- Quando você está utilizando telnet segura (SSL) e trabalhando com certificados que não são assinados por um CA conhecido, cada cliente deve incluir o certificado CA na lista de CAs confiáveis do Emulador de Conexão do Host.
- A opção NOSNAEXT de TELNETPARMS do TCP/IP pode ser necessária para desativar as extensões funcionais do SNA. Se NOSNAEXT for especificado, o servidor telnet TN3270 não negociará as funções de resolução de contenção e de detecção do SNA.



---

## Capítulo 13. Configurando o SSL e a Autenticação X.509

Essa seção é fornecida para ajudá-lo com alguns problemas comuns que podem ser encontrados durante a configuração da Secure Socket Layer (SSL) ou durante a verificação ou modificação de uma configuração existente. Essa seção também fornece uma configuração de amostra para suportar que os usuários se autenticuem com um certificado X.509.

Comunicação segura significa garantir que seu parceiro de comunicação seja o que alega ser e transmitir informações de forma que dificulte a interceptação e leitura dos dados por terceiros. O SSL fornece essa capacidade em uma rede TCP/IP. Funciona utilizando certificados digitais para se identificar e um protocolo de chave pública para criptografar a comunicação. Consulte o Guia de Administrador de Segurança *Servidor de Segurança RACF* (SA22-7683) para obter mais informações sobre certificados digitais e o protocolo de chave pública usado por SSL.

As ações necessárias para configurar as comunicações SSL para o Developer for System z variam de site para site, dependendo das necessidades exatas, do método de comunicação RSE usado e do que já está disponível no site.

Nessa seção, clonaremos as definições de RSE atuais, para que possamos ter uma segunda conexão de daemon RSE que usará SSL. Também criaremos nossos próprios certificados de segurança a serem usados pelas diferentes partes da conexão RSE.

- “Decida Usar o SSL ou TLS Como o Método de Criptografia” na página 184
- “Decidir Onde Armazenar Chaves Privadas e Certificados” na página 184
- “Criar um Conjunto de Chaves com o RACF” na página 185
- “Clonar a Configuração RSE Existente” na página 186
- “Atualizar rsed.envvars para Ativar a Coexistência” na página 187
- “Atualizar ssl.properties para Ativar SSL” na página 187
- “Ativar SSL Criando um Novo Daemon RSE” na página 187
- “Testar a Conexão” na página 188
- “(Opcional) Incluir Suporte de Autenticação de Cliente X.509” na página 191
- “(Opcional) Criar um Banco de Dados de Chaves com gskkyman” na página 191
- “(Opcional) Criar um Keystore com keytool” na página 193

Ao longo desta seção, uma convenção de nomenclatura uniforme é utilizada:

- Certificado: rdzrse
- Armazenamento de chaves e certificados: rdzssl.\*
- Senha: rsessl
- ID de usuário do Daemon: stcrse

Algumas tarefas descritas nas seções a seguir esperam que você esteja ativo no z/OS UNIX. Isso pode ser feito emitindo o comando do TSO **OMVS**. Use o comando **exit** para retornar ao TSO.

---

## Decida Usar o SSL ou TLS Como o Método de Criptografia

A variável `DSTORE_SSL_ALGORITHM` na diretiva `_RSE_JAVA_OPTS` de `rsed.envvars` permite escolher entre o SSL e sua Segurança da Camada de Transporte (TLS) sucessora como o método de criptografia, conforme documentado em "Definindo Parâmetros de Inicialização Java Extra com o `_RSE_JAVA_OPTS`" no *Guia de Configuração do Host* (S517-9094).

---

## Decidir Onde Armazenar Chaves Privadas e Certificados

Os certificados de identidade e as chaves de criptografia/descriptografia usadas pelo SSL são armazenados em um arquivo de chaves. Existem diferentes implementações deste arquivo de chaves, dependendo do tipo de aplicativo.

No entanto, todas as implementações seguem o mesmo princípio. Um comando gera um par de chaves (uma chave pública e uma chave privada associada). O comando agrupa então a chave pública em um certificado X.509 auto-assinado, que é armazenado como uma cadeia de certificados de elemento único. Essa cadeia de certificados e a chave privada são armazenadas como uma entrada (identificada por um alias) em um arquivo-chave.

O daemon RSE é um aplicativo SSL do Sistema e utiliza um arquivo de banco de dados de chaves. Esse banco de dados de chaves pode ser um arquivo físico criado por `gskkyman` ou um conjunto de chaves gerenciado pelo seu software de segurança compatível com SAF (por exemplo, RACF). O servidor RSE (que é iniciado pelo daemon) é um aplicativo Java SSL e usa um arquivo keystore criado por `keytool` ou um conjunto de chaves gerenciado pelo seu software de segurança.

*Tabela 44. Mecanismos de armazenamento de certificado SSL*

| Armazenamento de certificado | Criado e gerenciado por                 | Daemon RSE | Servidor RSE |
|------------------------------|-----------------------------------------|------------|--------------|
| conjunto de chaves           | Produto de segurança compatível com SAF | suportados | suportados   |
| banco de dados de chaves     | <code>gskkyman</code> do z/OS UNIX      | suportados | /            |
| keystore                     | <code>keytool</code> do Java            | /          | suportados   |

Para conectar por meio de SSL, é necessário o keystore e o banco de dados principal, como um arquivo z/OS UNIX ou um conjunto de chaves compatível com SAF:

- keystore (RACF ou `keytool`)
- banco de dados de chaves (RACF ou `gskkyman`)

### **Nota:**

- Conjuntos de chaves compatíveis com SAF é o método preferido para gerenciar certificados.
- Um certificado compartilhado poderá ser usado se o daemon RSE e o servidor RSE usarem o mesmo método de gerenciamento de certificado.
- O daemon RSE deve ser executado controlado pelo programa. O uso do SSL do Sistema implica que `SYS1.SIEALNKE` deve se tornar controlado pelo programa pelo software de segurança.
- Para executar um aplicativo SSL do Sistema (conexão daemon), o `SYS1.SIEALNKE` deve estar em `LINKLIST` ou em `STEPLIB`. Se você preferir o método `STEPLIB`, inclua a seguinte instrução no fim de `rsed.envvars`.

`STEPLIB=$STEPLIB:SYS1.SIEALNKE`

Porém, lembre-se de que:



- A utilização de STEPLIB no z/OS UNIX tem um impacto de desempenho negativo.
- Se uma biblioteca STEPLIB for autorizada pelo APF, todas serão autorizadas. As bibliotecas perderão sua autorização do APF se forem combinadas com as bibliotecas no STEPLIB não autorizadas.
- O SSL do Sistema utiliza o ICSF (Integrated Cryptographic Service Facility), se estiver disponível. O ICSF oferece suporte criptográfico a hardware que será usado, em vez de algoritmos de software do SSL do Sistema. Consulte *System SSL Programming* (SC24-5901) para obter informações adicionais.

Consulte *Security Server RACF Security Administrator's Guide* (SA22-7683) para obter informações sobre RACF e caracteres digitais. A documentação de gskkyman pode ser localizada em *System SSL Programming* (SC24-5901) e a documentação de keytool está disponível em <http://java.sun.com/j2se/1.5.0/docs/tooldocs/solaris/keytool.html>.

---

## Criar um Conjunto de Chaves com o RACF

Não execute esta etapa se utilizar o gskkyman para criar o banco de dados de chaves do daemon RSE e o keytool para criar o keystore do servidor RSE.

O comando **RACDCERT** instala e mantém chaves privadas e certificados no RACF. O RACF suporta várias chaves privadas e certificados para serem gerenciados como um grupo. Esses grupos são chamados anéis de chave.

Os certificados podem ser auto-assinados ou assinados por uma Autoridade de Certificação (CA). Um certificado assinado por uma CA significa que a CA garante que o proprietário do certificado é quem afirma ser. O processo de assinatura inclui as credenciais de CA (também um certificado) no certificado, tornando-o uma cadeia de certificados com vários elementos.

Ao usar um certificado assinado por uma CA, você pode evitar perguntas sobre validação confiável pelo cliente do Developer for System z, se o cliente já confiar na CA.

Consulte *Security Server RACF Command Language Reference* (SA22-7687) para obter detalhes sobre o comando **RACDCERT**.

```
permita que o daemon RSE acesse os certificados
RDEFINE FACILITY IRR.DIGTCERT.LIST UACC(NONE)
RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC(NONE)
PERMIT IRR.DIGTCERT.LIST CLASS(FACILITY) ACCESS(READ) ID(stcrse)
PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ACCESS(READ) ID(stcrse)

atualize para tornar as mudanças visíveis
SETROPTS RACLIST(FACILITY) REFRESH

crie certificado autoassinado
RACDCERT ID(stcrse) GENCERT SUBJECTSDN(CN('rdz rse ssl') +
OU('rdz') O('IBM') L('Raleigh') SP('NC') C('US')) +
NOTAFTER(DATE(2017-05-21)) WITHLABEL('rdzrse') KEYUSAGE(HANDSHAKE)

(opcional) etapas adicionais necessárias para usar um certificado assinado
1. crie uma solicitação de assinatura para o certificado autoassinado
RACDCERT ID(stcrse) GENREQ (LABEL('rdzrse')) DSN(dsn)
2. envie a solicitação de assinatura para a CA de sua escolha
3. verifique se as credenciais de CA (também um certificado) já são conhecidas
RACDCERT CERTAUTH LIST
4. marque o certificado de CA como confiável
RACDCERT CERTAUTH ALTER(LABEL('CA cert')) TRUST
ou inclua o certificado de CA no banco de dados
RACDCERT CERTAUTH ADD(dsn) WITHLABEL('CA cert') TRUST
5. inclua o certificado assinado ao banco de dados;
isso substituirá o autoassinado
RACDCERT ID(stcrse) ADD(dsn) WITHLABEL('rdzrse') TRUST
NÃO exclua o certificado autoassinado antes de substituí-lo.
Se você fizer isso, perderá a chave privada fornecida com o certificado,
o que torna o certificado inútil.

RACDCERT ID(stcrse) ADDRING(rdzssl.racf)
RACDCERT ID(stcrse) CONNECT(LABEL('rdzrse') RING(rdzssl.racf) +
DEFAULT USAGE(PERSONAL))
```

```
etapa adicional necessária para usar um certificado assinado
6. inclua a autoridade de certificado ao conjunto de chaves
RACDCERT ID(stcrse) CONNECT(CERTAUTH LABEL('CA cert') +
RING(rdzssl.racf))
atualize para tornar as mudanças visíveis
SETROPTS RACLIST(DIGTCERT) REFRESH
```

A amostra anterior inicia criando os perfis necessários e permitindo que o ID de usuário STCRSE acesse os conjuntos de chaves e os certificados pertencentes a esse ID de usuário. O ID do usuário usado deve corresponder ao ID do usuário usado para executar o daemon do RSE SSL. A próxima etapa é criar um novo certificado auto-assinado com rótulo rdzrse. Não é necessária senha. Esse certificado é incluído em um anel de chaves recém-criado (rdzssl.racf). Assim como com o certificado, não é necessária senha para o anel de chave. As etapas necessárias para usar um certificado assinado também estão listadas.

Observe que o certificado CA usado para assinar seu certificado pode, por sua vez, também ser assinado por outro certificado CA, de nível mais alto. Se isso acontecer, o certificado CA de nível mais alto também deverá ser incluído no conjunto de chaves. Esse processo se repete até que o certificado CA de nível mais alto seja um certificado CA raiz, que é sempre um certificado autoassinado.

O resultado pode ser verificado com as opções list e listring a seguir:

```
RACDCERT ID(stcrse) LIST
Informações do certificado digital para o usuário STCRSE:

Rótulo: rdzrse
ID do Certificado: 2QjW10Xi0sXZ1aaEqZmihUBA
Status: TRUST
Data de Início: 24/05/2007 0h
Data de Encerramento: 21/05/2017 23h59min59s
Número de Série:
>00<
Nome do Emissor:
>CN=my CA.OU=rdz.O=IBM.L=Raleigh.SP=NC.C=US<
Nome do Assunto:
>CN=rdz rse ssl.OU=rdz.O=IBM.L=Raleigh.SP=NC.C=US<
Tipo de Chave Privada: não ICSF
Tamanho da Chave Privada: 1024
Associações de Anel:
 Proprietário do Anel: STCRSE
 Anel:
 >rdzssl.racf<

RACDCERT ID(stcrse) LISTRING(rdzssl.racf)
Informações de anel digital para o usuário STCRSE:

Anel:
>rdzssl.racf<
Certificate Label Name Cert Owner USAGE DEFAULT

rdzrse ID(STCRSE) PERSONAL YES
CA cert CERTAUTH CERTAUTH NO
```

## Clonar a Configuração RSE Existente

Nesta etapa, uma nova instância dos arquivos de configuração do RSE é criada, para que a configuração SSL possa ser executada paralelamente com a(s) existente(s). Os comandos de amostra a seguir esperam que os arquivos de configuração estejam em /etc/rdz/, que é o local padrão usado em "Configuração de customização" no *Guia de Configuração do Host* (SC23-7658).

```
$ cd /etc/rdz
$ mkdir ssl
$ cp rsed.envvars ssl
$ cp ssl.properties ssl
$ ls ssl
rsed.envvars ssl.properties
```

Os comandos do z/OS UNIX listados no exemplo anterior criam um subdiretório chamado ssl e o preenchem com os arquivos de configuração que precisam de mudanças. Podemos compartilhar os outros arquivos de configuração, o diretório de instalação e os componentes do MVS, porque não são específicos do SSL.

Ao reutilizar a maioria dos arquivos de configuração existentes, podemos nos concentrar nas alterações realmente necessárias para configurar o SSL e evitar fazer a configuração completa do RSE novamente. (Por exemplo, podemos evitar a definição de um novo local para ISPF.conf.)

---

## Atualizar rsed.envvars para Ativar a Coexistência

Até agora, as definições são uma cópia exata da configuração atual, o que implica que os logs do novo daemon RSE sobreporão os arquivos de log atuais do servidor. O RSE também precisa saber onde localizar os arquivos de configuração que não foram copiados para o diretório ssl. Os dois problemas podem ser tratados por mudanças secundárias em rsed.envvars.

```
$ oedit /etc/rdz/ssl/rsed.envvars
-> change: _RSE_RSED_PORT=4047
-> change: _Ddaemon.Log=/var/rdz/logs/ssl
-> change: _Duser.log=/var/rdz/logs/ssl
-> add at the END:
-- NEEDED TO FIND THE REMAINING CONFIGURATION FILES
CFG_BASE=/etc/rdz
CLASSPATH=.:$CFG_BASE:$CLASSPATH
--
```

As mudanças no exemplo anterior definem um novo local de log (que será criado pelo daemon RSE se o local do log não existir). As mudanças também atualizam o CLASSPATH para que os processos RSE do SSL procurem arquivos de configuração primeiramente no diretório atual (/etc/rdz/ssl) e, em seguida, procurem no diretório original (/etc/rdz).

---

## Atualizar ssl.properties para Ativar SSL

Atualizando ssl.properties, o RSE é orientado a iniciar o uso da comunicação criptografada por SSL.

```
$ oedit /etc/rdz/ssl/ssl.properties
-> change: enable_ssl=true
-> uncomment and change: daemon_keydb_file=rdzssl.racf
-> uncomment and change: daemon_key_label=rdzrse
-> uncomment and change: server_keystore_file=rdzssl.racf
-> uncomment and change: server_keystore_label=rdzrse
-> uncomment and change: server_keystore_type=JCERACFKS
```

As mudanças no exemplo anterior ativam o SSL e informam ao daemon RSE e ao servidor RSE que o certificado (compartilhado) deles está armazenado com o rótulo de rdzrse no conjunto de chaves rdzssl.racf. A palavra-chave JCERACFKS informa ao servidor RSE que um conjunto de chaves compatível com SAF é usado como keystore.

Observe que o SSL do Sistema (usado pelo daemon) sempre usa o ICSF, a interface com o hardware criptográfico System z, quando disponível. Para poder compartilhar as definições de daemon com o servidor usando o ICSF, especifique server\_keystore\_type JCECCARACFKS. Aqui, um conjunto de chaves compatível com SAF também é usado como armazenamento de chaves públicas, mas a chave privada é armazenada no ICSF. Conforme documentado no *Cryptographic Services ICSF Administrator's Guide* (SA22-7521), o ICSF usa perfis nas classes de segurança CSFKEYS e CSFSERV para controlar quem pode usar chaves e serviços criptográficos.

---

## Ativar SSL Criando um Novo Daemon RSE

Conforme já mencionado, criaremos uma segunda conexão que utilizará SSL, o que significa a criação de um novo daemon do RSE. O daemon do RSE pode ser uma tarefa iniciada ou uma tarefa do usuário. O método de tarefa do usuário para configuração (teste) inicial será usado. As instruções a seguir esperam que a JCL de amostra esteja em FEK.#CUST.PROCLIB(RSED), que é o local padrão usado em "Configuração de customização" no *Guia de Configuração do Host* (SC23-7658):

1. Crie um novo membro FEK.#CUST.PROCLIB(RSEDSSL) e copie na JCL de amostra FEK.#CUST.PROCLIB(RSED).
2. Customize RSEDSSL incluindo uma placa de tarefa na parte superior e uma instrução exec na parte inferior. Forneça também o local dos arquivos de configuração relacionados a SSL (/etc/rdz/ssl), conforme descrito na seguinte amostra de código. Observe que forçamos o uso do ID de usuário STCRSE, pois esse ID de usuário recebeu a autoridade de acesso apropriada para certificados e conjuntos de chaves em uma etapa anterior.

```
//RSEDSSL JOB CLASS=A,MSGCLASS=A,MSGLEVEL=(1,1),USER=STCRSE
//*
//* RSE DAEMON - SSL
//*
//RSED PROC TMPDIR=,
// PORT=,
// IVP=, * 'IVP' to do an IVP test
// CNFG='/etc/rdz/ssl',
// HOME='/usr/lpp/rdz'
//*
//RSED EXEC PGM=BPXBATSL,REGION=0M,TIME=NOLIMIT,
// PARM='PGM &HOME./bin/rsed.sh &IVP -C&CNFG -P&PORT -T&TMPDIR'
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
// PEND
//*
//RSED EXEC RSED
//*
```

*Figura 36. RSEDSSL - Tarefa do usuário do daemon RSE para SSL*

**Nota:** O ID de usuário designado à tarefa RSEDSSL deve ter as mesmas autorizações que o daemon RSE original. O perfil FACILITY BPX.SERVER e o perfil PTKTDATA IRRPTAUTH.FEKAPPL.\* são elementos-chave aqui.

---

## Testar a Conexão

A configuração do host SSL é completa e o daemon RSE para SSL pode ser iniciado ao enviar a tarefa FEK.#CUST.PROCLIB(RSEDSSL) criada anteriormente.

A nova configuração pode agora ser testada conectando-se com o cliente Developer for System z. Como criamos uma nova configuração para ser usada pelo SSL (clonando uma existente), uma nova conexão deverá ser definida no cliente utilizando-se a porta 4047 para o daemon RSE.

Na conexão, o host e o cliente começarão com alguma troca para configurar um caminho seguro. Parte dessa troca é o intercâmbio de certificados. Se o cliente Developer for System z não reconhecer o certificado do host ou a CA que o assinou, o cliente Developer for System z perguntará ao usuário se é possível confiar nesse certificado.

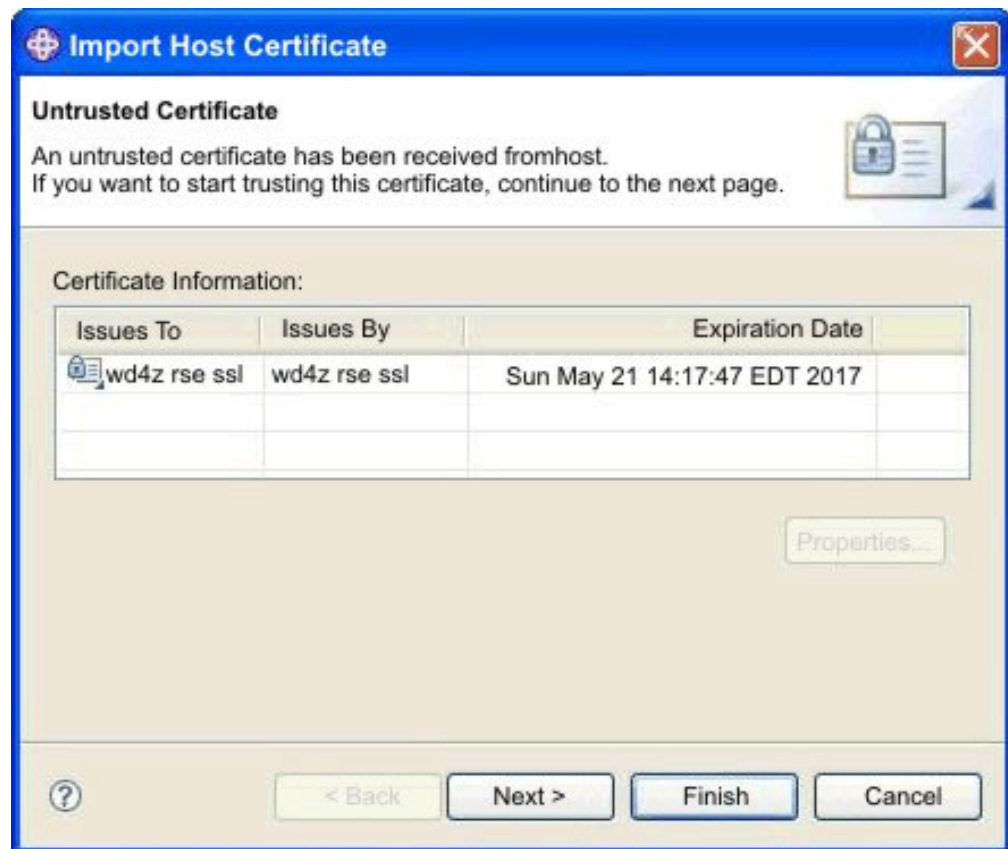


Figura 37. Diálogo Importar Certificado do Host

Clicando no botão Concluir, o usuário pode aceitar esse certificado como confiável; depois disso, a inicialização da conexão continuará.

**Nota:** O daemon RSE e o servidor RSE podem utilizar dois locais de certificados diferentes, resultando em dois certificados diferentes e, portanto, em duas confirmações.

Quando um certificado é conhecido do cliente, esse diálogo não é mostrado novamente. A lista de certificados confiáveis pode ser gerenciada selecionando **Janela > Preferências... > Sistemas Remotos > SSL**, que mostra o seguinte diálogo:



Figura 38. Diálogo Preferências - SSL

Se a comunicação SSL falhar, o cliente retornará uma mensagem de erro.  
Informações adicionais estão disponíveis nos diferentes arquivos de log do servidor

e do usuário, conforme descrito em “Criação de Log de Daemon RSE e de Conjunto de Encadeamento” na página 166 e “criação de logs do usuário do RSE” na página 167.

---

## (Opcional) Incluir Suporte de Autenticação de Cliente X.509

O daemon RSE suporta que os próprios usuários se autenticuem com um certificado X.509. Usar a comunicação criptografada SSL é um pré-requisito para essa função por ser uma extensão para a autenticação de host com um certificado usado no SSL.

Há várias maneiras de fazer a autenticação de certificado para um usuário, conforme descrito em “Autenticação de cliente usando certificados X.509” na página 31. As próximas etapas documentam a configuração necessária para suportar o método em que o software de segurança autentica o certificado utilizando a extensão de certificado HostIdMappings.

1. Altere o certificado que identifica a Autoridade de Certificação (CA) usado para assinar o certificado do cliente para um certificado de CA altamente confiável. Embora o status TRUST seja suficiente para a validação de certificado, é feita uma mudança para HIGHTRUST por ser usado para a parte de autenticação de certificado do processo de logon.

```
RACDCERT CERTAUTH ALTER(LABEL('HighTrust CA')) HIGHTRUST
```

2. Inclua o certificado de CA no conjunto de chaves `rdzssl.racf` para que esteja disponível para validar os certificados de cliente.

```
RACDCERT ID(stcrse) CONNECT(CERTAUTH LABEL('HighTrust CA') +
RING(rdzssl.racf))
```

Isso conclui a configuração do software de segurança para o certificado de CA.

3. Defina um recurso (formato `IRR.HOST.hostname`) na classe `SERVAUTH` para o nome do host, `CDFMVS08.RALEIGH.IBM.COM`, definido na extensão `HostIdMappings` do certificado do cliente.

```
RDEFINE SERVAUTH IRR.HOST.CDFMVS08.RALEIGH.IBM.COM UACC(NONE)
```

4. Conceda ao ID do usuário da tarefa iniciada do RSE, `STCRSE`, acesso a esse recurso com autoridade `READ`.

```
PERMIT IRR.HOST.CDFMVS08.RALEIGH.IBM.COM CLASS(SERVAUTH) +
ACCESS(READ) ID(stcrse)
```

5. Ative suas mudanças para a classe `SERVAUTH`. Use o primeiro comando se a classe `SERVAUTH` ainda não estiver ativa. Use o segundo para atualizar uma configuração ativa.

```
SETROPTS CLASSACT(SERVAUTH) RACLIST(SERVAUTH)
ou
SETROPTS RACLIST(SERVAUTH) REFRESH
```

Isso conclui a configuração do software de segurança para a extensão `HostIdMappings`.

6. Reinicie a tarefa iniciada do RSE para começar a aceitar logons de clientes usando os certificados X.509.

---

## (Opcional) Criar um Banco de Dados de Chaves com gskkyman

Não execute esta etapa se você usar um conjunto de chaves compatível com SAF para o banco de dados principal do daemon RSE.

`gskkyman` é um programa z/OS UNIX baseado em shell e orientado por menus, que cria, preenche e gerencia um arquivo z/OS UNIX que contém chaves privadas, pedidos de certificado e certificados. Esse arquivo z/OS UNIX é chamado de banco de dados de chaves.



**Nota:** As seguintes instruções podem ser necessárias para configurar o ambiente para gskkyman. Consulte *System SSL Programming* (SC24-5901) para obter mais informações sobre isso.

```
PATH=$PATH:/usr/lpp/gskssl/bin
export NLSPATH=/usr/lpp/gskssl/lib/nls/msg/En_US.IBM-1047/%N:$NLSPATH
export STEPLIB=$STEPLIB:SYS1.SIEALNKE

$ cd /etc/rdz/ssl
$ gskkyman Menu do Banco de Dados

 1 - Criar novo banco de dados

Digite o número da opção: 1
Digite o nome do banco de dados de chaves (pressione ENTER para retornar ao menu): rdzssl.kdb
Digite a senha do banco de dados (pressione ENTER para retornar ao menu): rsessl
Digite novamente a senha do banco de dados: rsessl
Digite a expiração da senha em dias (pressione ENTER para nenhuma expiração):
Digite o comprimento do registro do banco de dados (pressione ENTER para utilizar 2500):

Banco de dados de chaves /etc/rdz/ssl/rdzssl.kdb criado.

Pressione ENTER para continuar.

 Menu do Key Management

 6 - Criar um certificado auto-assinado

Digite o número da opção (pressione ENTER para retornar ao menu anterior): 6

 Tipo de Certificado

 5 - Certificado do usuário ou do servidor com chave RSA de 1024 bits

Selecione o tipo de certificado (pressione ENTER para retornar ao menu): 5
Digite o rótulo (pressione ENTER para retornar ao menu): rdzrse
Digite o nome do assunto para o certificado
 Nome comum (necessário): rdz rse ssl
 Unidade organizacional (opcional): rdz
 Organização (necessário): IBM
 Cidade/Localidade (opcional): Raleigh
 Estado/Provincia (opcional): NC
 País/Região (2 caracteres - necessário): US
Digite o número de dias que o certificado permanecerá válido (padrão 365): 3650

Digite 1 para especificar nomes alternativos de assunto ou 0 para continuar: 0

Aguarde

Certificado criado.

Pressione ENTER para continuar.

 Menu do Key Management

 0 - Sair do programa

Digite o número da opção (pressione ENTER para retornar ao menu anterior): 0
$ ls -l rdzssl.*
total 152
-rw----- 1 IBMUSER SYS1 35080 May 24 14:24 rdzssl.kdb
-rw----- 1 IBMUSER SYS1 80 May 24 14:24 rdzssl.rdb
$ chmod 644 rdzssl.*
$ ls -l rdzssl.*
-rw-r--r-- 1 IBMUSER SYS1 35080 May 24 14:24 rdzssl.kdb
-rw-r--r-- 1 IBMUSER SYS1 80 May 24 14:24 rdzssl.rdb
```

A amostra anterior inicia criando um banco de dados de chaves chamado `rdzssl.kdb` com a senha `rsessl`. Quando o banco de dados existir, ele será preenchido por meio da criação de um novo certificado auto-assinado, válido durante 10 anos (sem contar os dias extras). O certificado é armazenado com o rótulo `rdzrse` e com a mesma senha (`rsessl`) usada para o banco de dados de chaves (esse é um requisito do RSE).

`gskkyman` aloca o banco de dados de chaves com uma máscara de bits de permissão 600 (muito segura) (só o proprietário tem acesso). A menos que o daemon utilize o mesmo ID do usuário que o criador do banco de dados de chaves, as permissões devem ser configuradas menos restritivas. 644 (o proprietário tem leitura/gravação, todos têm leitura) é uma máscara útil para o comando `chmod`.

O resultado pode ser verificado ao selecionar a opção **Mostrar Informações do Certificado** no submenu **Gerenciar Chaves e Certificados**, como a seguir:

```
$ gskkyman

 Menu do Banco de Dados

 2 - Abrir banco de dados

Digite o número da opção: 2
```

```

Digite o nome do banco de dados de chaves (pressione ENTER para retornar ao menu): rdzssl.kdb
Digite a senha do banco de dados (pressione ENTER para retornar ao menu): rsessl

Menu do Key Management

1 - Gerenciar chaves e certificados

Digite o número da opção (pressione ENTER para retornar ao menu anterior): 1

Lista de Chaves e Certificados

1 - rdzrse

Digite o número do rótulo (ENTER para retornar ao menu de seleção, p para lista anterior): 1

Menu Chave e Certificado

1 - Mostrar informações do certificado

Digite o número da opção (pressione ENTER para retornar ao menu anterior): 1

Informações do Certificado

Rótulo: rdzrse
ID do Registro: 14
ID do Registro do Emissor: 14
Confiável: Sim
Versão: 3
Número serial: 45356379000ac997
Nome do emissor: rdz rse ssl
rdz
IBM
Raleigh
NC
Nome do assunto: rdz rse ssl
rdz
IBM
Raleigh
NC
Data de efetivação: 24/05/2007
Data de expiração: 21/05/2017
Algoritmo de chave pública: rsaEncryption
Tamanho da chave pública: 1024
Algoritmo de assinatura: sha1WithRsaEncryption
ID exclusivo do emissor: Nenhum
ID exclusivo do assunto: Nenhum
Número de extensões: 3

Digite 1 para exibir extensões, 0 para retornar ao menu: 0

Menu Chave e Certificado

0 - Sair do programa

Digite o número da opção (pressione ENTER para retornar ao menu anterior): 0

```

A amostra `ssl.properties` a seguir mostra que as diretivas `daemon_*` são diferentes da amostra do conjunto de chaves SAF anterior.

```

$ oedit /etc/rdz/ssl/ssl.properties
-> change: enable_ssl=true
-> uncomment and change: daemon_keydb_file=rdzssl.kdb
-> uncomment and change: daemon_keydb_password=rsessl
-> uncomment and change: daemon_key_label=rdzrse
-> uncomment and change: server_keystore_file=rdzssl.racf
-> uncomment and change: server_keystore_label=rdzrse
-> uncomment and change: server_keystore_type=JCERACFKS

```

As mudanças anteriores ativam o SSL e informam ao daemon RSE que o certificado está armazenado com o rótulo `rdzrse` no banco de dados de chaves `rdzssl.kdb` com a senha `rsessl`. O servidor RSE ainda está usando um conjunto de chaves compatível com SAF.

---

## (Opcional) Criar um Keystore com keytool

Não execute esta etapa se você utilizar um conjunto de chaves compatível com SAF para o keystore do servidor RSE.

"keytool -genkey" gera um par de chaves privadas e um certificado auto-assinado correspondente que são armazenados como uma entrada (identificada por um alias) em um arquivo keystore (novo).

**Nota:** Java deve ser incluído nos diretórios de procura de comando. A instrução a seguir pode ser necessária para executar o `keytool`, em que `/usr/lpp/java/J5.0` é o diretório em que Java está instalado: `PATH=$PATH:/usr/lpp/java/J5.0/bin`

Todas as informações podem ser transmitidas como um parâmetro, mas devido às limitações no comprimento da linha de comandos, será necessária uma certa interatividade, como a seguir:

```
$ cd /etc/rdz/ssl
$ keytool -genkey -alias rdzrse -validity 3650 -keystore rdzssl.jks -storepass
rsessl -keypass rsessl
Qual é o seu nome e sobrenome?
[Desconhecido]: rdz rse ssl
Qual é o nome de sua unidade organizacional?
[Desconhecido]: rdz
Qual é o nome de sua organização?
[Desconhecido]: IBM
Qual é o nome de sua cidade ou localidade?
[Desconhecido]: Raleigh
Qual é o nome de seu estado ou província?
[Desconhecido]: NC
Qual é o código do país de duas letras para esta unidade?
[Desconhecido]: US
CN=rdz rse ssl, OU=rdz, O=IBM, L=Raleigh, ST=NC, C=US está correto? (digite "sim"
ou "não")
[não]: sim
$ ls -l rdzssl.*
-rw-r--r-- 1 IBMUSER SYS1 1224 May 24 14:17 rdzssl.jks
```

O certificado autoassinado criado no exemplo anterior é válido durante aproximadamente 10 anos (não contando o dia 29 de fevereiro). Ele é armazenado em `/etc/rdz/ssl/rdzssl.jks` utilizando o alias `rdzrse`. Sua senha (`rsessl`) é idêntica à senha do armazenamento de chaves, que é um requisito para o RSE.

O resultado pode ser verificado com a opção `-list`, como a seguir:

```
$ keytool -list -alias rdzrse -keystore rdzssl.jks -storepass rsessl -v
Nome do alias: rdzrse
Data de criação: 24 de maio de 2007
Tipo de entrada: keyEntry
Comprimento da cadeia de certificados: 1
Certificado 1:
Proprietário: CN=rdz rse ssl, OU=rdz, O=IBM, L=Raleigh, ST=NC, C=US
Emissor: CN=rdz rse ssl, OU=rdz, O=IBM, L=Raleigh, ST=NC, C=US
Número serial: 46562b2b
Válido de: 24/5/07 14h17 até: 21/5/17 14h17
Impressões digitais do certificado:
MD5: 9D:6D:F1:97:1E:AD:5D:B1:F7:14:16:4D:9B:1D:28:80
SHA1: B5:E2:31:F5:B0:E8:9D:01:AD:2D:E6:82:4A:E0:B1:5E:12:CB:10:1C
```

A amostra `ssl.properties` a seguir mostra que as diretivas `server_*` são diferentes da amostra do conjunto de chaves SAF anterior.

```
$ oedit /etc/rdz/ssl/ssl.properties
-> change: enable_ssl=true
-> uncomment and change: daemon_keydb_file=rdzssl.racf
-> uncomment and change: daemon_key_label=rdzrse
-> uncomment and change: server_keystore_file=rdzssl.jks
-> uncomment and change: server_keystore_password=rsessl
-> uncomment and change: server_keystore_label=rdzrse
-> optionally uncomment and change: server_keystore_type=JKS
```

As mudanças anteriores ativam o SSL e informam ao servidor RSE que o certificado está armazenado com o rótulo `rdzrse` no armazenamento de chaves `rdzssl.jks` com a senha `rsessl`. O daemon RSE ainda está usando um conjunto de chaves compatível com SAF.

---

## Capítulo 14. Configurando o AT-TLS

Essa seção é fornecida para ajudá-lo com alguns problemas comuns que podem ser encontrados durante a configuração da Segurança da Camada de Transporte Transparente do Aplicativo (AT-TLS) ou durante a verificação ou modificação de uma configuração existente.

O protocolo do Transport Layer Security (TLS) definido em RFC 2246 fornece privacidade de comunicações pela Internet. Semelhante ao seu predecessor Secure Socket Layer (SSL), o protocolo permite que aplicativos cliente e servidor se comuniquem de uma forma projetada para evitar escuta de terceiros, violação e falsificação de mensagens. O Application Transparent Transport Layer Security (AT-TLS) consolida a implementação de TLS para aplicativos baseados em z/OS em um local, permitindo que todos os aplicativos suportem a criptografia baseada em TLS sem o conhecimento do protocolo TLS. Consulte *Communications Server IP - Guia de Configuração* (SC31-8775) para obter mais informações sobre o AT-TLS.

O Depurador Integrado do IBM Rational Developer for System z conta com o AT-TLS para comunicação criptografada com o cliente, porque os dados para a sessão de depuração não fluem pelo mesmo canal que outras comunicações do cliente com o host do Developer for System z.

As ações necessárias para configurar o AT-TLS variarão de acordo com o site, dependendo das necessidades exatas e dependendo do que já está disponível no site.

As informações desta seção mostram como configurar o Agente de Diretiva de TCP/IP que gerencia o AT-TLS e define uma política para o uso pelo Depurador Integrado do Developer for System z em um sistema z/OS 1.13, com suporte para TLS v1.2.

1. “Configurando syslogd” na página 196
2. “Configuração do AT-TLS no PROFILE.TCPIP” na página 196
3. “Tarefa Iniciada do Policy Agent” na página 196
4. “Configuração do Policy Agent” na página 197
5. “Política AT-TLS” na página 197
6. “Atualizações de Segurança do AT-TLS” na página 199
7. “Ativação da Política AT-TLS” na página 201

Ao longo desta seção, uma convenção de nomenclatura uniforme é utilizada:

- Porta do Debug Manager para comunicação externa: 5335
- ID do usuário do Debug Manager: stcdm
- ID do usuário do Policy Agent: pagent
- Certificado: dbgmgr
- Armazenamento de chaves e certificados: dbgmgr.racf

Algumas tarefas descritas nas seções a seguir esperam que você esteja ativo no z/OS UNIX. Isso pode ser feito emitindo o comando do TSO **OMVS**. Use o comando **oedit** para editar arquivos no z/OS UNIX. Use o comando **exit** para retornar ao TSO.

---

## Configurando syslogd

A documentação do TCP/IP recomenda escrever as mensagens do Policy Agent no syslog do z/OS UNIX em vez de usar o arquivo de log padrão. AT-TLS sempre gravará as mensagens no syslog do z/OS UNIX.

Para fazer isso, o daemon do syslog do z/OS UNIX, `syslogd`, deve estar configurado e ativo. Também será necessário um mecanismo para controlar o tamanho dos arquivos de log criados pelo `syslogd`.

As atualizações de arquivo de configuração de amostra a seguir podem ser usadas para configurar e iniciar `syslogd`, com um mecanismo de gerenciamento de arquivos de log simples (apague os logs existentes quando z/OS UNIX iniciar e crie novos na inicialização de `syslogd`).

- `/etc/services`

```
syslog 514/udp
```

- `/etc/syslog.conf`

```
/etc/syslog.conf - control output of syslogd
1. todos os arquivos serão impressos em /tmp/syslog.auth.log
auth.* /tmp/syslog.auth.log
2. todas as mensagens de erro são impressas em /tmp/syslog.error.log
*.err /tmp/syslog.error.log
3. todas as mensagens de depuração e acima são impressas em /tmp/syslog.debug.log
*.debug /tmp/syslog.debug.log
Os nomes de arquivos devem existir antes de o daemon syslog ser iniciado,
a menos que a opção de inicialização -c seja usada
```

- `/etc/rc`

```
Inicie o daemon SYSLOGD para a criação de log
(limpe os logs antigos)
sed -n '/^#/s/.* \(.*)/l/p' /etc/syslog.conf | xargs -i rm {}
(crie novos logs e inclua o ID do usuário do emissor da mensagem)
_BPX_JOBNAME='SYSLOGD' /usr/sbin/syslogd -cuf /etc/syslog.conf &
sleep 5
```

---

## Configuração do AT-TLS no PROFILE.TCPIP

O suporte do AT-TLS é ativado pelo parâmetro TTLS na instrução `TCPCONFIG` no conjunto de dados `PROFILE.TCPIP`. AT-TLS é gerenciado pelo Policy Agent, que deve estar ativo para permitir impingir a política AT-TLS. Como o Policy Agent deve aguardar que o TCP/IP esteja ativo, a instrução `AUTOSTART` em `PROFILE.TCPIP` é um bom local para acionar a inicialização deste servidor.

Esses requisitos resultam nas mudanças a seguir para `PROFILE.TCPIP`, muitas vezes denominado `TCPIP.TCPPARMS(TCPPROF)`.

```
TCPCONFIG TTLS ; Requerido para AT-TLS
AUTOLOG
PAGENT ; POLICY AGENT, requerido para AT-TLS
ENDAUTOLOG
```

---

## Tarefa Iniciada do Policy Agent

Como mencionado anteriormente, AT-TLS é gerenciado pelo Policy Agent, que pode ser iniciado como uma tarefa iniciada. Use o JCL a seguir para criar `SYS1.PROCLIB(PAGENT)`, usando o arquivo de configuração padrão e o local de log recomendado (`SYSLOGD`). As definições necessárias no software de segurança são discutidas posteriormente.

```
//PAGENT PROC PRM='-L SYSLOGD' * '' or '-L SYSLOGD'
/**
/** TCP/IP POLICY AGENT
/**
/** default cfg file: /etc/pagent.conf (PARM) (envar)
/** default log file: /tmp/pagent.log (-C) (PAGENT_CONFIG_FILE)
/** default log size: 300,3 (3x 300KB files) (-L) (PAGENT_LOG_FILE)
/**
//PAGENT EXEC PGM=PAGENT,REGION=0M,TIME=NOLIMIT,
// PARM='ENVAR("TZ=EST5DST")/&PRM'
//SYSPRINT DD SYSOUT=*
//SYSOUT DD SYSOUT=*
/**
```

## Configuração do Policy Agent

O Policy Agent impinge as políticas relacionadas a TCP/IP, criadas pelo administrador de TCP/IP. Ele gerencia políticas para o AT-TLS, chamadas TTLS, mas também para outros serviços, como o IPSec. O Policy Agent usa um arquivo de configuração para saber quais políticas devem ser impingidas e onde elas podem ser localizadas. O arquivo de configuração padrão é `/etc/pagent.conf`, mas um local diferente pode ser especificado no JCL da tarefa iniciada do Policy Agent.

```
#
Informações de configuração do TCP/IP Policy Agent.
#
TTLSConfig /etc/pagent.ttls.conf
Especifica o caminho de um arquivo de políticas TTLS que possui instruções específicas de
pilha.
#
#TcpImage TCPIP /etc/pagent.conf
Se nenhuma instrução TcpImage for especificada, todas as políticas serão instaladas
à pilha TCP/IP padrão.
#
#LogLevel 31
A soma dos valores a seguir que representam os níveis de log:
LOGL_SYSERR 1
LOGL_OBJERR 2
LOGL_PROTERR 4
LOGL_WARNING 8
LOGL_EVENT 16
LOGL_ACTION 32
LOGL_INFO 64
LOGL_ACNTING 128
LOGL_TRACE 256
Nível de Log 31 é o nível de log padrão.
#
#Codepage IBM-1047
Especifique a página de códigos EBCDIC a ser usada para a leitura de todos os arquivos de
configuração e arquivos de definição de política. IBM-1047 é a página de códigos padrão.
```

Esse arquivo de configuração de amostra especifica onde o Policy Agent pode localizar a política de TTLS. Ele usa os valores padrão do Policy Agent para outras instruções.

## Política AT-TLS

Uma política TTLS descreve as regras desejadas de AT-TLS. Como definido no arquivo de configuração do Policy Agent, a política do TTLS está localizada em `/etc/pagent.ttls.conf`. As definições necessárias no software de segurança são discutidas posteriormente.

Este exemplo mostra uma política de duas regras, bastante simples, que ativa o suporte SSL v3, TLS v1, TLS v1.1 e TLS v1.2 para caminhos de comunicação suportados pelo Depurador Integrado Developer for System z, Debug Manager e Cliente de Análise. Como definido no arquivo de configuração do Policy Agent, a política do TTLS está localizada em `/etc/pagent.ttls.conf`.

```
##
Informações de configuração do TCP/IP Policy Agent AT-TLS.
##
##-----
TTLSRule RDz_Debug_Manager
(
 LocalPortRange 5335
 Direction Inbound
 TTLSGroupActionRef grp_Production
 TTLSEnvironmentActionRef act_RDz_Debug_Manager
)
##-----
```

```

TTLSEnvironmentAction act_RDz_Debug_Manager
{
 HandshakeRole Server
 TTLSKeyRingParms
 {
 Keyring dbgmgr.racf # Keyring must be owned by the Debug Manager
 }
 TTLSEnvironmentAdvancedParms
 {
 ## TLSV1.2 apenas para z/OS 2.1 e superior
 # TLSV1.2 On # SSLv3, TLSv1 & TLSv1.1 estão ativos por padrão
 }
}
#####
TTLSRule RDz_Debug_Probe-Client
{
 RemotePortRange 8001
 Direção Saída
 TTLSGroupActionRef grp_Production
 TTLSEnvironmentActionRef act_RDz_Debug_Probe-Client
}
#####
TTLSEnvironmentAction act_RDz_Debug_Probe-Client
{
 HandshakeRole Cliente
 TTLSKeyRingParms
 {
 Keyring *AUTH*/* # conjunto de chaves virtuais que possuem certificados de CA
 }
 TTLSEnvironmentAdvancedParms
 {
 ## TLSV1.2 apenas para z/OS 2.1 e superior
 # TLSV1.2 On # SSLv3, TLSv1 & TLSv1.1 estão ativos por padrão
 }
}
#####
TTLSGroupAction grp_Production
{
 TTLSEnabled On
 ## TLSV1.2z0S1.13 apenas para z/OS 1.13
 TTLSGroupAdvancedParmsRef TLSv1.2z0S1.13
 Trace 3 # Registrar Erros para syslogd & IP joblog
 #Trace 254 # Registrar tudo para syslogd
}
#####
TTLSGroupAdvancedParms TLSv1.2z0S1.13
{
 Envfile /etc/pagent.ttls.TLS1.2z0S1.13.env
}

```

Uma política TTLS permite um intervalo amplo de filtros para especificar quando uma regra é aplicada.

O Debug Manager é um servidor que recebe conexões de entrada do Mecanismo de Depuração na porta 5335. Essas informações são capturadas na regra RDz\_Debug\_Manager.

Como SSL e TLS requerem o uso de um certificado do servidor, especifique que o Policy Manager deve usar os certificados do conjunto de chaves dbgmgr.racf, que é de propriedade do ID do usuário da tarefa iniciada do Debug Manager. Por padrão, o suporte de TLS v1.2 está desativado, então essa política o ativa explicitamente.

Quando a Análise de Depuração é iniciada com a opção Ambiente de Linguagem (LE) TEST(,,,TCP/IP&&ipaddress%8001:\*), é indicado que não se use o Debug Manager, mas entre em contato diretamente com o cliente do Developer for System z na porta 8001. Isso implica, de uma perspectiva do TCP/IP, que a Análise de Depuração baseada no host é um cliente contatando um servidor(a UI de Depuração) no cliente do Developer for System z. Essas informações são capturadas na regra RDz\_Debug\_Probe-Client.

Com o host sendo um cliente TCP/IP, o Policy Manager precisará de uma maneira de validar o certificado do servidor apresentado pela UI de Depuração. Em vez de usar um conjunto de chaves denominado uniformemente para todos os usuários que possam requerer uma sessão de depuração criptografada, estamos usando o conjunto de chaves virtuais CERTAUTH do RACF (\*AUTH\*/\*). Esse conjunto de chaves virtuais contém os certificados públicos das Autoridades de Certificação (CAs) e podem ser usados se a UI de Depuração apresentar um certificado do servidor assinado por uma das CAs confiáveis.



Observe que, para políticas mais complexas, você deve usar o IBM Configuration Assistant para z/OS Communications Server. Essa é uma ferramenta baseada em GUI que fornece uma interface guiada para a configuração das funções de rede baseadas em políticas de TCP/IP e está disponível como uma tarefa em IBM z/OS Management Facility (z/OSMF), e como um aplicativo de estação de trabalho independente.

## Considerações sobre o TLS v1.2

O suporte de TLS v1.2 tornou-se disponível no z/OS 2.1, e está desativado por padrão. Essa política mostra o comando (TLSV1.2 ON) para ativá-lo explicitamente, mas a linha está comentada visto que o sistema de destino está usando o z/OS 1.13.

Ao aplicar os dois APARs a seguir, o suporte de TLS v1.2 é incluído ao z/OS 1.13:

- System SSL APAR OA39422
- Communications Server (AT-TLS) APAR PM62905

O z/OS 1.13 System SSL, que é usado pelo AT-TLS para implementar a comunicação criptografada, requer alguns parâmetros adicionais para o suporte do TLS v1.2. Estes são fornecidos por meio da política AT-TLS usando um arquivo com variáveis de ambiente do System SSL, /etc/pagent.ttls.TLS1.2zOS1.13.env.

```
#
Inclua o suporte de TLSv1.2 para AT-TLS
requer z/OS 1.13 com OA39422 e PM62905
#
GSK_RENEGOTIATION=ALL
GSK_PROTOCOL_TLSV1_2=ON
```

---

## Atualizações de Segurança do AT-TLS

Há várias atualizações necessárias para sua configuração de segurança para AT-TLS funcionar apropriadamente. Esta seção possui os comandos RACF de amostra para executar a configuração necessária.

Como mencionado em “Tarefa Iniciada do Policy Agent” na página 196, você usa uma tarefa iniciada para executar o Policy Agent. Isso requer a definição de um ID do usuário de tarefa iniciada e um perfil na classe STARTED.

```
defina o ID do usuário da tarefa iniciada
a permissão BPX.DAEMON é necessária para o UID não zero
ADDUSER PAGENT DFLTGRP(SYS1) OMVS(UID(0) SHARED HOME('/')) +
NAME('TCP/IP POLICY AGENT') NOPASSWORD

defina a tarefa iniciada
RDEFINE STARTED PAGENT.* STDATA(USER(PAGENT) GROUP(SYS1)) +
DATA('TCP/IP POLICY AGENT')

atualize para tornar as mudanças visíveis
SETROPTS RACLIST(STARTED) REFRESH
```

Defina um perfil denominado MVS.SERVMgr.PAGENT na classe OPERCMDS e forneça o acesso PAGENT CONTROL do ID do usuário para ele. O perfil restringe quem pode iniciar o Policy Agent. Se o perfil não estiver definido e o acesso a ele for evitado através de um perfil genérico, PAGENT não poderá iniciar o Policy Agent, o que evitará a inicialização de pilha TCP/IP.

```
restrinja a inicialização do policy agent
RDEFINE OPERCMDS MVS.SERVMgr.PAGENT UACC(NONE) +
DATA('restrict startup of policy agent')
PERMIT MVS.SERVMgr.PAGENT CLASS(OPERCMDS) ACCESS(CONTROL) ID(PAGENT)

atualize para tornar as mudanças visíveis
SETROPTS RACLIST(OPERCMDS) REFRESH
```

Como mencionado em “Configuração do AT-TLS no PROFILE.TCPIP” na página 196, o Policy Agent é iniciado após a inicialização do TCP/IP. Isso significa que há uma (pequena) janela em que os aplicativos podem usar a pilha TCP/IP sem

impingir a política de TTLS. Defina o perfil EZB.INITSTACK.\*\* na classe SERVAUTH para evitar o acesso à pilha durante esse período de tempo, exceto para aplicativos com acesso READ ao perfil. É necessário permitir o acesso de um conjunto limitado de aplicativos administrativos ao perfil para assegurar a inicialização integral da pilha, como documentado em “Controle de acesso de inicialização à pilha TCP/IP” em *Communications Server IP - Guia de Configuração* (SC31-8775).

```
bloqueie o acesso de pilha entre a pilha e a disponibilidade de AT-TLS
SETROPTS GENERIC(SERVAUTH)
SETROPTS CLASSACT(SERVAUTH) RACLIST(FACILITY)
RDEFINE SERVAUTH EZB.INITSTACK.** UACC(NONE)
Policy Agent
PERMIT EZB.INITSTACK.** CLASS(SERVAUTH) ACCESS(READ) ID(PAGENT)
OMPROUTE daemon
PERMIT EZB.INITSTACK.** CLASS(SERVAUTH) ACCESS(READ) ID(OMPROUTE)
agente e sub-agentes SNMP
PERMIT EZB.INITSTACK.** CLASS(SERVAUTH) ACCESS(READ) ID(OSNMPD)
PERMIT EZB.INITSTACK.** CLASS(SERVAUTH) ACCESS(READ) ID(IOBSNMP)
daemon NAME
PERMIT EZB.INITSTACK.** CLASS(SERVAUTH) ACCESS(READ) ID(NAMED)

atualize para tornar as mudanças visíveis
SETROPTS RACLIST(SERVAUTH) REFRESH
```

(Opcional) O comando **pasearch** do z/OS UNIX exhibe as definições de políticas ativas. Defina o perfil EZB.PAGENT.\*\* na classe SERVAUTH para restringir o acesso ao comando **pasearch**.

```
restrinja o acesso ao comando pasearch
RDEFINE SERVAUTH EZB.PAGENT.** UACC(NONE) +
DATA('restrict access to pasearch command')
PERMIT EZB.PAGENT.** CLASS(SERVAUTH) ACCESS(READ) ID(tcpadmin)

atualize para tornar as mudanças visíveis
SETROPTS RACLIST(SERVAUTH) REFRESH
```

Como mencionado em “Política AT-TLS” na página 197, Debug Manager precisa de um certificado para que o AT-TLS possa configurar a comunicação criptografada SSL ou TLS em nome do Debug Manager. Esses comandos de amostra criam um novo certificado denominado **dbgmgr**, armazenado em um conjunto de chaves RACF denominado **dbgmgr.racf**. Ambos o certificado e o conjunto de chaves são de propriedade do STCDBM, o ID do usuário da tarefa iniciada do Debug Manager.

```
permita que o Debug Manager acesse os certificados
#RDEFINE FACILITY IRR.DIGTCERT.LIST UACC(NONE)
#RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC(NONE)
PERMIT IRR.DIGTCERT.LIST CLASS(FACILITY) ACCESS(READ) ID(stcdbm)
PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ACCESS(READ) ID(stcdbm)

atualize para tornar as mudanças visíveis
SETROPTS RACLIST(FACILITY) REFRESH

crie certificado autoassinado
RACDCERT ID(stcdbm) GENCERT SUBJECTSDN(CN('RDz Debug Manager') +
OU('RTP labs') O('IBM') L('Raleigh') SP('NC') C('US')) +
NOTAFTER(DATE(2015-12-31)) KEYUSAGE(HANDSHAKE) WITHLABEL('dbgmgr')

(opcional) etapas adicionais necessárias para usar um certificado assinado
1. crie uma solicitação de assinatura para o certificado autoassinado
RACDCERT ID(stcdbm) GENREQ (LABEL('dbgmgr')) DSN(dsn)
2. envie a solicitação de assinatura para a CA de sua escolha
3. verifique se as credenciais de CA (também um certificado) já são conhecidas
RACDCERT CERTAUTH LIST
4. marque o certificado de CA como confiável
RACDCERT CERTAUTH ALTER(LABEL('CA cert')) TRUST
ou inclua o certificado de CA no banco de dados
RACDCERT CERTAUTH ADD(dsn) WITHLABEL('CA cert') TRUST
5. inclua o certificado assinado ao banco de dados;
isso substituirá o autoassinado
RACDCERT ID(stcdbm) ADD(dsn) WITHLABEL('dbgmgr') TRUST
NÃO exclua o certificado autoassinado antes de substituí-lo.
Se você fizer isso, perderá a chave privada fornecida com o certificado,
o que torna o certificado inútil.

crie o conjunto de chaves
RACDCERT ID(stcdbm) ADDRING(dbgmgr.racf)

inclua o certificado ao conjunto de chaves
RACDCERT ID(stcdbm) CONNECT(LABEL('dbgmgr') +
RING(dbgmgr.racf) USAGE(PERSONAL) DEFAULT)

etapa adicional necessária para usar um certificado assinado
6. inclua o certificado de autoridade de certificação ao conjunto de chaves
RACDCERT ID(stcdbm) CONNECT(CERTAUTH LABEL('CA cert') +
RING(dbgmgr.racf))

atualize para tornar as mudanças visíveis
SETROPTS RACLIST(DIGTCERT) REFRESH
```

A política AT-TLS também documenta o uso do conjunto de chaves virtuais CERTAUTH para validação do certificado do servidor apresentado pela UI de Depuração no cenário Cliente de Análise. Isso implica que o certificado CA usado pelo Debug UI é confiável por seu host z/OS.

```
verifique se as credenciais de CA (também um certificado) já são conhecidas
RACDCERT CERTAUTH LIST
marque o certificado de CA como confiável
RACDCERT CERTAUTH ALTER(LABEL('CA cert')) TRUST
ou inclua o certificado de CA no banco de dados
RACDCERT CERTAUTH ADD(dsn) WITHLABEL('CA cert') TRUST

atualize para tornar as mudanças visíveis
SETROPTS RACLIST(DIGTCERT) REFRESH
```

Use os comandos a seguir para verificar sua configuração:

```
verifique a configuração da tarefa iniciada
LISTGRP SYSL OMVS
LISTUSER PAGENT OMVS
RLIST STARTED PAGENT.* ALL STDATA

verifique a permissão de inicialização do Policy Agent
RLIST OPERCMDS MVS.SERVGR.PAGENT ALL

verifique a proteção initstack
RLIST SERVAUTH EZB.INITSTACK.** ALL

verifique a proteção pasearch
RLIST SERVAUTH EZB.PAGENT.** ALL

verifique a configuração do certificado
RACDCERT CERTAUTH LIST(LABEL('CA cert'))
RACDCERT ID(stcdbm) LIST(LABEL('dbgmgr'))
RACDCERT ID(stcdbm) LISTRING(dbgmgr.racf)
```

---

## Ativação da Política AT-TLS

A configuração de AT-TLS está concluída e a política será ativada no próximo carregamento inicial de programas do sistema. Siga estas etapas para iniciar o uso da política sem um carregamento inicial de programas:

### 1. Ative o suporte de AT-TLS na pilha TCP/IP.

Crie um arquivo obey TCP/IP, por exemplo, TCPIP.TCPPARMS(OBEY), com o conteúdo a seguir:

```
TCPCONFIG TTLS
```

Ative-o com este comando do operador:

```
V TCPIP,,OBEY,TCPIP.TCPPARMS(OBEY)
```

Verifique o resultado verificando esta mensagem do console:

```
EZZ4249I stackname INSTALLED TTLS POLICY HAS NO RULES
```

### 2. Inicie o Policy Agent.

Emita o comando do operador:

```
S PAGENT
```

Verifique o resultado verificando a mensagem do console:

```
EZD1586I PAGENT HAS INSTALLED ALL LOCAL POLICIES FOR stackname
```

### 3. Reinicie o Debug Manager para interromper todas as sessões ativas não criptografadas.

Emita os comandos do operador:

```
P DBGMR
S DBBMGR
```



---

## Capítulo 15. Configurando o TCP/IP

Essa seção é fornecida para ajudá-lo com alguns problemas comuns que podem ser encontrados durante a configuração do TCP/IP ou durante a verificação ou modificação de uma instalação existente.

Consulte *Communications Server: IP Configuration Guide* (SC31-8775) e *Communications Server: IP Configuration Reference* (SC31-8776) para obter informações adicionais sobre a configuração do TCP/IP.

---

### Dependência do nome do host

Com o uso de APPC para o serviço TSO Commands, o Developer for System z depende de o TCP/IP ter o nome do host correto quando for inicializado. Isto significa que o TCP/IP diferente e os arquivos de configuração do Resolver devem ser configurados corretamente.

Você pode testar sua configuração TCP/IP com o Installation Verification Program (IVP) do fekfivpt. O comando deve retornar uma saída como nesta amostra (\$ é o prompt do z/OS UNIX):

```
$ fekfivpt

Quarta-feira, 2 de julho de 2008, 13h11min54s EDT
uid=1(USERID) gid=0(GROUP)
utilizando /etc/rdz/rsed.envvars

Configuração do resolvidor TCP/IP (ordem de procura do z/OS UNIX):

Inicialização de Rastreo do Resolvidor Concluída -> 2008/07/02 13:11:54.745964

res_init Resolver values:
Global Tcp/Ip Dataset = None
Default Tcp/Ip Dataset = None
Local Tcp/Ip Dataset = /etc/resolv.conf
Translation Table = Default
UserId/JobName = USERID
Caller API = LE C Sockets
Caller Mode = EBCDIC
(L) DataSetPrefix = TCP/IP
(L) HostName = CDFMVS08
(L) TcpIpJobName = TCP/IP
(L) DomainOrigin = RALEIGH.IBM.COM
(L) NameServer = 9.42.206.2
 9.42.206.3
(L) NsPortAddr = 53 (L) ResolverTimeout = 10
(L) ResolveVia = UDP (L) ResolverUdpRetries = 1
(*) Options NDots = 1
(*) SockNoTestStor
(*) AlwaysWto = NO (L) MessageCase = MIXED
(*) LookUp = DNS LOCAL

res_init Succeeded
res_init Started: 2008/07/02 13:11:54.755363
res_init Ended: 2008/07/02 13:11:54.755371

MVS TCP/IP NETSTAT CS V1R9 TCP/IP Name: TCP/IP 13:11:54
Tcpi started at 01:28:36 on 06/23/2008 with IPv6 enabled

endereço IP do host:

hostName=CDFMVS08
hostAddr=9.42.112.75
bindAddr=9.42.112.75
localAddr=9.42.112.75

Êxito, os endereços correspondem
```

---

### Compreendendo os Resolvedores

O resolvidor atua em nome de programas como um cliente que acessa servidores de nomes para resolução de nome para endereço e de endereço para nome. Para resolver a consulta do programa solicitante, o resolvidor pode acessar os servidores de nomes disponíveis, utilize definições locais (por exemplo,

/etc/resolv.conf, /etc/hosts, /etc/ipnodes, HOSTS.SITEINFO, HOSTS.ADDRINFO ou ETC.IPNODES) ou utilize uma combinação delas.

Quando o espaço de endereços do resolvidor é iniciado, ele lê um conjunto de dados de configuração do resolvidor opcional apontado pelo cartão SETUP DD no procedimento JCL do resolvidor. Se as informações de configuração não forem fornecidas, o resolvidor usará a ordem de procura nativa aplicável do MVS ou do z/OS UNIX sem nenhuma informação de GLOBALTCPIPDATA, DEFAULTTCPIPDATA, GLOBALIPNODES, DEFAULTIPNODES ou COMMONSEARCH.

---

## Compreendendo as Ordens de Procura das Informações de Configuração

É importante compreender o ordem de procura dos arquivos de configuração usados pelas funções TCP/IP, e quando você pode sobrescrever a ordem de procura padrão com variáveis de ambiente, JCL ou outras variáveis fornecidas. Este conhecimento permite acomodar o conjunto de dados local e padrões de nomenclatura de arquivos HFS, e é útil conhecer o conjunto de dados da configuração ou o arquivo HFS em uso ao diagnosticar problemas.

Outro ponto importante a ser observado é que quando uma ordem de procura é aplicada para qualquer arquivo de configuração, a procura finaliza com o primeiro arquivo localizado. Portanto, podem ocorrer resultados inesperados se você colocar informações de configuração em um arquivo que nunca é encontrado, pois outros arquivos aparecem antes na ordem de procura, ou porque o arquivo não está incluído na ordem de procura escolhida pelo aplicativo.

Ao procurar por arquivos de configuração, você pode informar explicitamente ao TCP/IP onde estão a maioria dos arquivos de configuração utilizando instruções DD nos procedimentos JCL ou configurando variáveis de ambiente. Caso contrário, você pode deixar o TCP/IP determinar dinamicamente o local dos arquivos de configuração, com base nas ordens de procura documentadas em *Communications Server: IP Configuration Guide* (SC31-8775).

O componente de configuração da pilha do TCP/IP utiliza o TCPIP.DATA durante a inicialização da pilha do TCP/IP para determinar o HOSTNAME da pilha. Para obter seu valor, a ordem de procura do ambiente do z/OS UNIX é usada.

**Nota:** Use o recurso do resolvidor de rastreamento para determinar que os valores de TCPIP.DATA estão sendo usados pelo resolvidor e de onde eles foram lidos. Para obter informações sobre como iniciar o rastreamento dinamicamente, consulte *Communications Server: IP Diagnosis Guide* (GC31-8782). Depois que o rastreamento for ativado, emita um comando TSO **NETSTAT HOME** e um comando shell **netstat -h** do z/OS UNIX para exibir os valores. A emissão de um PING de um nome de host do TSO e a partir do shell do z/OS UNIX também mostra a atividade de qualquer servidor DNS que possa estar configurado.

---

## Ordens de Procura Usadas no Ambiente do z/OS UNIX

O arquivo ou tabela específico que é procurado pode ser um conjunto de dados MVS ou um arquivo HFS, dependendo das definições de configuração do resolvidor e da presença de determinados arquivos no sistema.

## Arquivos de Base da Configuração do Resolvedor

O arquivo de base da configuração do resolvedor contém instruções TCPIP.DATA. Além das diretivas do resolvedor, ele é referido para determinar, entre outras coisas, o prefixo do conjunto de dados (valor da instrução DATASETPREFIX) a ser usado ao tentar acessar alguns arquivos de configuração especificados nesta seção.

A ordem de procura usada para acessar o arquivo de configuração do resolvedor de base é a seguinte:

### 1. GLOBALTCPIPDATA

Se definido, o valor da instrução de configuração GLOBALTCPIPDATA do resolvedor é usado (consulte também “Compreendendo os Resolvedores” na página 203). A procura continua por um arquivo de configuração adicional. A procura finaliza com o próximo arquivo localizado.

### 2. O valor da variável de ambiente RESOLVER\_CONFIG

O valor da variável de ambiente é usado. Esta procura falhará se o arquivo não existir ou estiver alocado exclusivamente em outro lugar.

### 3. /etc/resolv.conf

### 4. Cartão //SYSTCPD DD

O conjunto de dados alocado para o SYSTCPD de nome DD é usado. No ambiente z/OS UNIX, um processo-filho não possui acesso ao DD SYSTCPD. Isto porque a alocação de SYSTCPD não é herdada do processo-pai por meio das chamadas de função fork() ou exec.

### 5. userid.TCPIP.DATA

userid é o ID do usuário associado ao ambiente de segurança atual (espaço de endereço, tarefa ou encadeamento).

### 6. jobname.TCPIP.DATA

jobname é o nome especificado na instrução JOB da JCL para tarefas em lote ou o nome do procedimento para um procedimento iniciado.

### 7. SYS1.TCPPARMS(TCPDATA)

### 8. DEFAULTTCPIPDATA

Se definido, o valor da instrução de configuração DEFAULTTCPIPDATA do resolvedor é usado (consulte também “Compreendendo os Resolvedores” na página 203).

### 9. TCPIP.TCPIP.DATA

## Tabelas de Conversão

As tabelas de conversão (EBCDIC-to-ASCII e ASCII-to-EBCDIC) são consultadas para determinar os conjuntos de dados de conversão a serem usados. A ordem de procura usada para acessar o arquivo de configuração é a seguinte. A ordem de procura termina quando o primeiro arquivo é localizado:

### 1. O valor da variável de ambiente X\_XLATE. O valor da variável de ambiente é o nome da tabela de conversão produzida pelo comando CONVXLAT do TSO.

### 2. userid.STANDARD.TCPXLBIN

userid é o ID do usuário associado ao ambiente de segurança atual (espaço de endereço ou tarefa/encadeamento).

### 3. jobname.STANDARD.TCPXLBIN

jobname é o nome especificado na instrução JOB da JCL para tarefas em lote ou o nome do procedimento para um procedimento iniciado.

### 4. hlq.STANDARD.TCPXLBIN



hlq representa o valor da instrução DATASETPREFIX especificada no arquivo de base da configuração do resolvidor (se localizado); caso contrário, hlq é TCPIP por padrão.

5. Se nenhuma tabela for encontrada, o resolvidor usará uma tabela padrão codificada permanentemente, idêntica à tabela listada no membro do conjunto de dados SEZATCPX(STANDARD).

## Tabelas do Host Local

Por padrão, o resolvidor primeiro tenta utilizar qualquer servidor de nomes de domínios configurado para pedidos de resolução. Se o pedido de resolução não puder ser satisfeito, as tabelas do host local são usadas. O comportamento do resolvidor é controlado pelas instruções TCPIP.DATA.

As instruções do resolvidor TCPIP.DATA definem se e como os servidores de nomes de domínios devem ser usados. A instrução LOOKUP TCPIP.DATA também pode ser usada para controlar como os servidores de nomes de domínios e as tabelas do host local são usadas. Para obter mais informações sobre instruções TCPIP.DATA, consulte *Communications Server: IP Configuration Reference* (SC31-8776).

O resolvidor utiliza a ordem de procura exclusiva Ipv4 para obter informações de nomes de sites incondicionalmente para chamadas de API getnetbyname. A ordem de procura exclusiva de Ipv4 para informações de nome de site é a seguinte. A procura termina quando o primeiro arquivo é localizado:

1. O valor da variável de ambiente **X\_SITE**  
O valor da variável de ambiente é o nome do arquivo de informações HOSTS.SITEINFO criado pelo comando **MAKESITE** do TSO.
2. O valor da variável de ambiente **X\_ADDR**  
O valor da variável de ambiente é o nome do arquivo de informações HOSTS.ADDRINFO criado pelo comando **MAKESITE** do TSO.
3. **/etc/hosts**
4. **userid.HOSTS.SITEINFO**  
userid é o ID do usuário associado ao ambiente de segurança atual (espaço de endereço ou tarefa/encadeamento).
5. **jobname.HOSTS.SITEINFO**  
jobname é o nome especificado na instrução JOB da JCL para tarefas em lote ou o nome do procedimento para um procedimento iniciado.
6. **hlq.HOSTS.SITEINFO**  
hlq representa o valor da instrução DATASETPREFIX especificada no arquivo de base da configuração do resolvidor (se localizado); caso contrário, hlq é TCPIP por padrão.

---

## Aplicando Estas Informações de Configuração ao Developer for System z

Conforme informado anteriormente, o Developer for System z depende de o TCP/IP ter o nome de host correto quando inicializado, ao utilizar APPC. Isto significa que o TCP/IP diferente e os arquivos de configuração do Resolver devem ser configurados corretamente.

O exemplo a seguir tem como foco algumas tarefas de configuração para o TCP/IP e o Resolvedor. Observe que isso não abrange uma configuração completa do TCP/IP ou do Resolver, ela destaca alguns aspectos principais que podem ser aplicáveis no seu site:

1. Na JCL a seguir, é possível ver que o TCP/IP usará SYS1.TCPPARMS(TCPDATA) para determinar o nome do host da pilha.

```
//TCP/IP PROC PARMS='CTRACE(CTIEZB00)',PROF=TCPPROF,DATA=TCPDATA
/*
/* TCP/IP NETWORK
/*
//TCP/IP EXEC PGM=EZBTCP/IP,REGION=OM,TIME=1440,PARM=&PARMS
//PROFILE DD DISP=SHR,DSN=SYS1.TCPPARMS(&PROF)
//SYSTCPD DD DISP=SHR,DSN=SYS1.TCPPARMS(&DATA)
//SYSPRINT DD SYSOUT=*,DCB=(RECFM=VB,LRECL=132,BLKSIZE=136)
//ALGPRINT DD SYSOUT=*,DCB=(RECFM=VB,LRECL=132,BLKSIZE=136)
//CFGPRINT DD SYSOUT=*,DCB=(RECFM=VB,LRECL=132,BLKSIZE=136)
//SYSOUT DD SYSOUT=*,DCB=(RECFM=VB,LRECL=132,BLKSIZE=136)
//CEEDUMP DD SYSOUT=*,DCB=(RECFM=VB,LRECL=132,BLKSIZE=136)
//SYSERROR DD SYSOUT=*
```

2. SYS1.TCPPARMS(TCPDATA) informa que o nome do sistema desejado é o nome do host e para não usar um servidor de nomes de domínio (DNS); todos os nomes serão resolvidos através da consulta de tabela do site.

```
; HOSTNAME especifica o nome do host TCP deste sistema. Se não
; especificado, o HOSTNAME padrão será o nome do nó especificado
; no membro IEFSSNxx PARMLIB.
;
; HOSTNAME
;
; DOMAINORIGIN especifica a origem do domínio que será anexado
; nos nomes dos hosts transmitidos para o resolvedor. Se um nome
; de host contiver
; algum ponto, então DOMAINORIGIN não será anexado
; ao nome do host.
;
; DOMAINORIGIN RALEIGH.IBM.COM
;
; NSINTERADDR especifica o endereço IP do servidor de nomes.
; LOOPBACK (14.0.0.0) especifica o servidor de nomes local. Se um servidor
; de nomes não será usado, então não codifique uma instrução NSINTERADDR.
; (Comente a linha NSINTERADDR abaixo). Isto fará com que todos os nomes
; sejam resolvidos por meio de consulta na tabela de sites.
;
; NSINTERADDR 14.0.0.0
;
; TRACE RESOLVER realizará um rastreamento completo de todas as consultas e
; fará com que as respostas do servidor de nomes ou tabelas de sites sejam
; gravadas no
; console do usuário. Este comando é destinado somente para
; finalidades de depuração.
;
; TRACE RESOLVER
```

3. No JCL do Resolvedor você vê que a instrução DD SETUP não é usada. Conforme mencionado em “Compreendendo os Resolvedores” na página 203, isto significa que GLOBALTCP/IPDATA e outras variáveis não serão usadas.

```
//RESOLVER PROC PARMS='CTRACE(CTIRES00)'
/*
/* IP NAME RESOLVER – START WITH SUB=MSTR
/*
//RESOLVER EXEC PGM=EZBREINI,REGION=OM,TIME=1440,PARM=&PARMS
//*SETUP DD DISP=SHR,DSN=USER.PROCLIB(RESSETUP),FREE=CLOSE
```

4. Se você assumir que a variável de ambiente RESOLVER\_CONFIG não está configurada, poderá ver na Tabela 45 na página 208 que o Resolvedor tentará usar /etc/resolv.conf como arquivo de configuração base.

```
TCPIPJOBNAME TCPIP
DomainOrigin RALEIGH.IBM.COM
HostName CDFMVS08
```

Conforme mencionado em “Ordens de Procura Usadas no Ambiente do z/OS UNIX” na página 204, o arquivo de base da configuração contém instruções TCPIP.DATA. Se o nome do sistema for CDFMVS08 (TCPDATA informou que o nome do sistema é usado como nome do host), você poderá ver que /etc/resolv.conf está em sincronismo com SYS1.TCPPARMS(TCPDATA) . Não há definições DNS, portanto a consulta à tabela de sites será usada.

5. A Tabela 45 na página 208 também informa que, se não for necessário fazer nada, usar a tabela de conversão ASCII-EBCDIC padrão.
6. Assumindo que o comando **MAKESITE** do TSO não seja usado (pode criar as variáveis X\_SITE e X\_ADDR), /etc/hosts será a tabela de sites usada para consulta de nomes.

```
Resolver /etc/hosts file cdfmvs08
9.42.112.75 cdfmvs08 # CDFMVS08 Host
9.42.112.75 cdfmvs08.raleigh.ibm.com # CDFMVS08 Host
127.0.0.1 localhost
```

O conteúdo mínimo deste arquivo é a informação sobre o sistema atual. Na amostra anterior, cdfmvs08 e cdfmvs08.raleigh.ibm.com são definidos como um nome válido para o endereço IP do sistema z/OS.

Se você estivesse usando servidor de nomes de domínio (DNS), o DNS conteria as informações de /etc/hosts, e /etc/resolv.conf e SYS1.TCPPARMS(TCPDATA) teriam instruções que identificariam o DNS para o sistema.

Para evitar confusão, e aconselhável manter os arquivos de configuração do TCP/IP e do Resolver em sincronismo um com o outro.

**Tabela 45. Definições locais disponíveis para o resolvidor**

| Descrição do Tipo do Arquivo                   | APIs afetadas                                                                                                                                                                                                                                             | Arquivos do Candidato                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Arquivos de Base da Configuração do Resolvedor | Todas as APIs                                                                                                                                                                                                                                             | <ol style="list-style-type: none"> <li>1. GLOBALTCPIPDATA</li> <li>2. variável de ambiente RESOLVER_CONFIG</li> <li>3. /etc/resolv.conf</li> <li>4. SYSTCPD DD-name</li> <li>5. userid.TCPIP.DATA</li> <li>6. jobname.TCPIP.DATA</li> <li>7. SYS1.TCPPARMS(TCPDATA)</li> <li>8. DEFAULTTCPIPDATA</li> <li>9. TCPIP.TCPIP.DATA</li> </ol>                                                                                                                                                                                          |
| Tabelas de Conversão                           | Todas as APIs                                                                                                                                                                                                                                             | <ol style="list-style-type: none"> <li>1. variável de ambiente X_XLATE</li> <li>2. userid.STANDARD.TCPXLBIN</li> <li>3. jobname.STANDARD.TCPXLBIN</li> <li>4. hlq.STANDARD.TCPXLBIN</li> <li>5. Tabela de conversão fornecida pelo resolvidor, membro STANDARD em SEZATCPX</li> </ol>                                                                                                                                                                                                                                             |
| Tabelas do Host Local                          | endhostent<br>endnetent<br>getaddrinfo<br>gethostbyaddr<br>gethostbyname<br>gethostent<br>GetHostNumber<br>GetHostResol<br>GetHostString<br>getnameinfo<br>getnetbyaddr<br>getnetbyname<br>getnetent<br>IsLocalHost<br>Resolve<br>sethostent<br>setnetent | IPv4 <ol style="list-style-type: none"> <li>1. variável de ambiente X_SITE</li> <li>2. variável de ambiente X_ADDR</li> <li>3. /etc/hosts</li> <li>4. userid.HOSTS.xxxxINFO</li> <li>5. jobname.HOSTS.xxxxINFO</li> <li>6. hlq.HOSTS.xxxxINFO</li> </ol> IPv6 <ol style="list-style-type: none"> <li>1. GLOBALIPNODES</li> <li>2. variável de ambiente RESOLVER_IPNODES</li> <li>3. userid.ETC.IPNODES</li> <li>4. jobname.ETC.IPNODES</li> <li>5. hlq.ETC.IPNODES</li> <li>6. DEFAULTIPNODES</li> <li>7. /etc/ipnodes</li> </ol> |

**Nota:** A Tabela 45 é uma cópia parcial de uma tabela em *Communications Server: IP Configuration Guide* (SC31-8775). Consulte esse manual para obter a tabela completa.

## O Endereço do Host Não É Resolvido Corretamente

Quando ocorrerem problemas nos quais o TCP/IP Resolver não pode resolver o endereço do host corretamente, muitas vezes isso é devido a um arquivo de configuração do resolvidor ausente ou incompleto. Uma indicação clara desse problema é a seguinte mensagem em lock.log:

```
clicntip(0.0.0.0) <> callerip(<endereço IP do host>)
```

Para verificar isso, execute o IVP de TCP/IP, fekfivpt, conforme descrito em "Verificação da instalação" no *Guia de Configuração do Host* (SC23-7658). A seção de configuração do resolvidor da saída será semelhante à seguinte amostra:

Inicialização de Rastreamento do Resolvidor Concluída -> 2008/07/02 13:11:54.745964

```
res_init Resolver values:
Global Tcp/Ip Dataset = None
Default Tcp/Ip Dataset = None
Local Tcp/Ip Dataset = /etc/resolv.conf
Translation Table = Default
UserId/JobName = USERID
Caller API = LE C Sockets
Caller Mode = EBCDIC
```

Certifique-se de que as definições no arquivo (ou conjunto de dados) referido pelo "Local Tcp/Ip Dataset" estejam corretas.

Esse campo ficará em branco se você não utilizar um nome padrão para o arquivo resolvidor de IP (utilizando a ordem de procura do z/OS UNIX). Nesse caso, inclua a seguinte instrução em `rsed.envvars`, em que <arquivo do resolvidor> ou <dados do resolvidor> representa o nome do arquivo do resolvidor de IP:

```
RESOLVER_CONFIG=<arquivo do resolvidor>
```

ou

```
RESOLVER_CONFIG='<conjunto de dados do resolvidor>'
```



# Bibliografia

## Publicações Referenciadas

As publicações a seguir são referenciadas neste documento:

*Tabela 46. Publicações Referenciadas*

| Título da publicação                                                                                 | Número da ordem | Referência             | Web site de referência                                                                                                                                                              |
|------------------------------------------------------------------------------------------------------|-----------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Diretório do Programa para IBM Rational Developer for System z                                       | GI11-8298       | Developer for System z | <a href="http://www-01.ibm.com/support/docview.wss?uid=swg27038517">http://www-01.ibm.com/support/docview.wss?uid=swg27038517</a>                                                   |
| Program Directory for IBM Rational Developer for System z Host Utilities                             | GI13-2864       | Developer for System z | <a href="http://www-01.ibm.com/support/docview.wss?uid=swg27038517">http://www-01.ibm.com/support/docview.wss?uid=swg27038517</a>                                                   |
| IBM Rational Developer for System zPré-requisitos                                                    | S517-9092       | Developer for System z | <a href="http://www-01.ibm.com/support/docview.wss?uid=swg27038517">http://www-01.ibm.com/support/docview.wss?uid=swg27038517</a>                                                   |
| IBM Rational Developer for System z Host Configuration Quick Start                                   | G517-9391       | Developer for System z | <a href="http://www-01.ibm.com/support/docview.wss?uid=swg27038517">http://www-01.ibm.com/support/docview.wss?uid=swg27038517</a>                                                   |
| IBM Rational Developer for System zGuia de Configuração do Host                                      | S517-9094       | Developer for System z | <a href="http://www-01.ibm.com/support/docview.wss?uid=swg27038517">http://www-01.ibm.com/support/docview.wss?uid=swg27038517</a>                                                   |
| IBM Rational Developer for System zReferência de Configuração do Host                                | S517-9857       | Developer for System z | <a href="http://www-01.ibm.com/support/docview.wss?uid=swg27038517">http://www-01.ibm.com/support/docview.wss?uid=swg27038517</a>                                                   |
| IBM Rational Developer for System z Guia do Utilitário de Configuração de Host                       | SC14-7282       | Developer for System z | <a href="http://www-01.ibm.com/support/docview.wss?uid=swg27038517">http://www-01.ibm.com/support/docview.wss?uid=swg27038517</a>                                                   |
| IBM Rational Developer for System z Messages and Codes                                               | SC14-7497       | Developer for System z | <a href="http://www-01.ibm.com/support/docview.wss?uid=swg27038517">http://www-01.ibm.com/support/docview.wss?uid=swg27038517</a>                                                   |
| IBM Rational Developer for System zRespostas a problemas comuns de manutenção e configuração de host | SC14-7373       | Developer for System z | <a href="http://www-01.ibm.com/support/docview.wss?uid=swg27038517">http://www-01.ibm.com/support/docview.wss?uid=swg27038517</a>                                                   |
| IBM Rational Developer for System z Common Access Repository Manager Developer's Guide               | SC23-7660       | Developer for System z | <a href="http://www-01.ibm.com/support/docview.wss?uid=swg27038517">http://www-01.ibm.com/support/docview.wss?uid=swg27038517</a>                                                   |
| IBM Rational Developer for System zPré-requisitos                                                    | S517-9092       | Developer for System z | <a href="http://www.ibm.com/software/rational/products/developer/systemz/library/index.html">http://www.ibm.com/software/rational/products/developer/systemz/library/index.html</a> |
| IBM Rational Developer for System z Host Configuration Quick Start                                   | G517-9391       | Developer for System z | <a href="http://www.ibm.com/software/rational/products/developer/systemz/library/index.html">http://www.ibm.com/software/rational/products/developer/systemz/library/index.html</a> |
| SCLM Developer Toolkit: Guia do Administrador                                                        | SC23-9801       | Developer for System z | <a href="http://www-01.ibm.com/support/docview.wss?uid=swg27038517">http://www-01.ibm.com/support/docview.wss?uid=swg27038517</a>                                                   |
| Usando APPC para fornecer serviços de comando TSO                                                    | SC14-7291       | White Paper            | <a href="http://www-01.ibm.com/support/docview.wss?uid=swg27038517">http://www-01.ibm.com/support/docview.wss?uid=swg27038517</a>                                                   |
| Usando Gateway do Cliente ISPF para fornecer serviços CARMA                                          | SC14-7292       | White Paper            | <a href="http://www-01.ibm.com/support/docview.wss?uid=swg27038517">http://www-01.ibm.com/support/docview.wss?uid=swg27038517</a>                                                   |
| Communications Server IP Configuration Guide                                                         | SC31-8775       | z/OS 1.13              | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                   |
| Communications Server IP Configuration Reference                                                     | SC31-8776       | z/OS 1.13              | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                   |
| Communications Server IP Diagnosis Guide                                                             | GC31-8782       | z/OS 1.13              | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                   |
| Communications Server IP System Administrator's Commands                                             | SC31-8781       | z/OS 1.13              | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                   |
| Communications Server SNA Network Implementation Guide                                               | SC31-8777       | z/OS 1.13              | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                   |
| Communications Server SNA Operations                                                                 | SC31-8779       | z/OS 1.13              | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                   |
| Cryptographic Services System SSL Programming                                                        | SC24-5901       | z/OS 1.13              | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                   |
| DFSMS Macro Instructions for Data Sets                                                               | SC26-7408       | z/OS 1.13              | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                   |
| DFSMS Using Data Sets                                                                                | SC26-7410       | z/OS 1.13              | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                   |
| Language Environment Customization                                                                   | SA22-7564       | z/OS 1.13              | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                   |
| Language Environment Debugging Guide                                                                 | GA22-7560       | z/OS 1.13              | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                   |
| Diagnóstico do MVS: Ferramentas e Auxílio de Serviço                                                 | GA22-7589       | z/OS 1.13              | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                   |
| MVS Initialization and Tuning Guide                                                                  | SA22-7591       | z/OS 1.13              | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                   |
| MVS Initialization and Tuning Reference                                                              | SA22-7592       | z/OS 1.13              | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                   |
| MVS JCL Reference                                                                                    | SA22-7597       | z/OS 1.13              | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                   |
| MVS Planning APPC/MVS Management                                                                     | SA22-7599       | z/OS 1.13              | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                   |
| MVS Planning Workload Management                                                                     | SA22-7602       | z/OS 1.13              | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                   |
| MVS System Commands                                                                                  | SA22-7627       | z/OS 1.13              | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                   |

**Tabela 46. Publicações Referenciadas (continuação)**

| Título da publicação                                | Número da ordem | Referência                 | Web site de referência                                                                                                                                                                                                                                            |
|-----------------------------------------------------|-----------------|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Security Server RACF Command Language Reference     | SA22-7687       | z/OS 1.13                  | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                                                                                                 |
| Security Server RACF Security Administrator's Guide | SA22-7683       | z/OS 1.13                  | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                                                                                                 |
| Customização de TSO/E                               | SA22-7783       | z/OS 1.13                  | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                                                                                                 |
| TSO/E REXX Reference                                | SA22-7790       | z/OS 1.13                  | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                                                                                                 |
| UNIX System Services Command Reference              | SA22-7802       | z/OS 1.13                  | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                                                                                                 |
| UNIX System Services Planning                       | GA22-7800       | z/OS 1.13                  | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                                                                                                 |
| UNIX System Services User's Guide                   | SA22-7801       | z/OS 1.13                  | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                                                                                                 |
| Utilizando os Serviços de Sistemas REXX e z/OS UNIX | SA22-7806       | z/OS 1.13                  | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                                                                                                 |
| Java™ Guia de Diagnóstico                           | SC34-6650       | Java 6.0                   | <a href="http://www.ibm.com/developerworks/java/jdk/diagnosis/">http://www.ibm.com/developerworks/java/jdk/diagnosis/</a>                                                                                                                                         |
| Guia do Usuário do Java SDK and Runtime Environment | /               | Java 6.0                   | <a href="http://www-03.ibm.com/servers/eserver/zseries/software/java/">http://www-03.ibm.com/servers/eserver/zseries/software/java/</a>                                                                                                                           |
| Resource Definition Guide                           | SC34-6430       | CICSTS 3.1                 | <a href="http://www-03.ibm.com/systems/z/os/zos/bkserv/zapplsbooks.html">http://www-03.ibm.com/systems/z/os/zos/bkserv/zapplsbooks.html</a>                                                                                                                       |
| Resource Definition Guide                           | SC34-6815       | CICSTS 3.2                 | <a href="http://www-03.ibm.com/systems/z/os/zos/bkserv/zapplsbooks.html">http://www-03.ibm.com/systems/z/os/zos/bkserv/zapplsbooks.html</a>                                                                                                                       |
| Resource Definition Guide                           | SC34-7000       | CICSTS 4.1                 | <a href="https://publib.boulder.ibm.com/infocenter/cicsts/v4r1/index.jsp?topic=/com.ibm.cics.ts.home.doc/library/library_html.html">https://publib.boulder.ibm.com/infocenter/cicsts/v4r1/index.jsp?topic=/com.ibm.cics.ts.home.doc/library/library_html.html</a> |
| Resource Definition Guide                           | SC34-7181       | CICSTS 4.2                 | <a href="https://publib.boulder.ibm.com/infocenter/cicsts/v4r2/index.jsp?topic=/com.ibm.cics.ts.home.doc/library/library_html.html">https://publib.boulder.ibm.com/infocenter/cicsts/v4r2/index.jsp?topic=/com.ibm.cics.ts.home.doc/library/library_html.html</a> |
| RACF Security Guide                                 | SC34-6454       | CICSTS 3.1                 | <a href="http://www-03.ibm.com/systems/z/os/zos/bkserv/zapplsbooks.html">http://www-03.ibm.com/systems/z/os/zos/bkserv/zapplsbooks.html</a>                                                                                                                       |
| RACF Security Guide                                 | SC34-6835       | CICSTS 3.2                 | <a href="http://www-03.ibm.com/systems/z/os/zos/bkserv/zapplsbooks.html">http://www-03.ibm.com/systems/z/os/zos/bkserv/zapplsbooks.html</a>                                                                                                                       |
| RACF Security Guide                                 | SC34-7003       | CICSTS 4.1                 | <a href="https://publib.boulder.ibm.com/infocenter/cicsts/v4r1/index.jsp?topic=/com.ibm.cics.ts.home.doc/library/library_html.html">https://publib.boulder.ibm.com/infocenter/cicsts/v4r1/index.jsp?topic=/com.ibm.cics.ts.home.doc/library/library_html.html</a> |
| RACF Security Guide                                 | SC34-7179       | CICSTS 4.2                 | <a href="https://publib.boulder.ibm.com/infocenter/cicsts/v4r2/index.jsp?topic=/com.ibm.cics.ts.home.doc/library/library_html.html">https://publib.boulder.ibm.com/infocenter/cicsts/v4r2/index.jsp?topic=/com.ibm.cics.ts.home.doc/library/library_html.html</a> |
| Referência de Linguagem                             | SC27-1408       | Enterprise COBOL para z/OS | <a href="http://www-03.ibm.com/systems/z/os/zos/bkserv/zapplsbooks.html">http://www-03.ibm.com/systems/z/os/zos/bkserv/zapplsbooks.html</a>                                                                                                                       |

Os Web sites a seguir são referidos neste documento:

**Tabela 47. Web Sites Referidos**

| Descrição                                              | Web site de referência                                                                                                                                                                                                                                                |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Developer for System z IBM Knowledge Center            | <a href="http://www-01.ibm.com/support/knowledgecenter/SSQ2R2_9.1.0/com.ibm.etools.getstart.wsentdev.doc/kc_version_welcome_rdz.html">http://www-01.ibm.com/support/knowledgecenter/SSQ2R2_9.1.0/com.ibm.etools.getstart.wsentdev.doc/kc_version_welcome_rdz.html</a> |
| Developer for System z Biblioteca                      | <a href="http://www-01.ibm.com/support/docview.wss?uid=swg27038517">http://www-01.ibm.com/support/docview.wss?uid=swg27038517</a>                                                                                                                                     |
| Developer for System z: Página Inicial                 | <a href="http://www-03.ibm.com/software/products/en/developerforsystemz/">http://www-03.ibm.com/software/products/en/developerforsystemz/</a>                                                                                                                         |
| Serviço recomendado do Developer for System z          | <a href="http://www-01.ibm.com/support/docview.wss?rs=2294&amp;context=SS2QJ2&amp;uid=swg27006335">http://www-01.ibm.com/support/docview.wss?rs=2294&amp;context=SS2QJ2&amp;uid=swg27006335</a>                                                                       |
| Solicitação de aprimoramento de Developer for System z | <a href="https://www.ibm.com/developerworks/support/rational/rfe/">https://www.ibm.com/developerworks/support/rational/rfe/</a>                                                                                                                                       |
| Biblioteca do z/OS na Internet                         | <a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>                                                                                                                                     |
| CICSTS IBM Knowledge Center                            | <a href="https://publib.boulder.ibm.com/infocenter/cicsts/v4r1/index.jsp">https://publib.boulder.ibm.com/infocenter/cicsts/v4r1/index.jsp</a>                                                                                                                         |
| IBM Tivoli Directory Server                            | <a href="http://www-01.ibm.com/software/tivoli/products/directory-server/">http://www-01.ibm.com/software/tivoli/products/directory-server/</a>                                                                                                                       |
| Plug-ins de Ferramentas de Determinação de Problemas   | <a href="http://www-01.ibm.com/software/awdtools/deployment/pdtplugins/">http://www-01.ibm.com/software/awdtools/deployment/pdtplugins/</a>                                                                                                                           |
| Informações de segurança Java                          | <a href="http://www.ibm.com/developerworks/java/jdk/security/">http://www.ibm.com/developerworks/java/jdk/security/</a>                                                                                                                                               |
| Download do Apache Ant                                 | <a href="http://ant.apache.org/">http://ant.apache.org/</a>                                                                                                                                                                                                           |
| Documentação do keytool Java                           | <a href="http://java.sun.com/j2se/1.5.0/docs/toolbox/solaris/keytool.html">http://java.sun.com/j2se/1.5.0/docs/toolbox/solaris/keytool.html</a>                                                                                                                       |
| Página inicial de suporte de CA                        | <a href="https://support.ca.com/">https://support.ca.com/</a>                                                                                                                                                                                                         |

## Publicações Informativas

As publicações a seguir podem ser úteis para você compreender os problemas de configuração dos componentes do sistema host necessários:

**Tabela 48. Publicações Informativas**

| Título da publicação                                                       | Número da ordem | Referência | Website de referência                                                   |
|----------------------------------------------------------------------------|-----------------|------------|-------------------------------------------------------------------------|
| ABCs do z/OS System Programming Volume 9 (z/OS UNIX)                       | SG24-6989       | Redbook    | <a href="http://www.redbooks.ibm.com/">http://www.redbooks.ibm.com/</a> |
| Guia do Programador de Sistema para: Workload Manager                      | SG24-6472       | Redbook    | <a href="http://www.redbooks.ibm.com/">http://www.redbooks.ibm.com/</a> |
| Implementação do TCP/IP Volume 1: Funções Base, Conectividade e Roteamento | SG24-7532       | Redbook    | <a href="http://www.redbooks.ibm.com/">http://www.redbooks.ibm.com/</a> |



*Tabela 48. Publicações Informativas (continuação)*

| <b>Título da publicação</b>                                                    | <b>Número da ordem</b> | <b>Referência</b> | <b>Website de referência</b>                                            |
|--------------------------------------------------------------------------------|------------------------|-------------------|-------------------------------------------------------------------------|
| TCPIP Implementation Volume 3: High Availability, Scalability, and Performance | SG24-7534              | Redbook           | <a href="http://www.redbooks.ibm.com/">http://www.redbooks.ibm.com/</a> |
| TCP/IP Implementation Volume 4: Security and Policy-Based Networking           | SG24-7535              | Redbook           | <a href="http://www.redbooks.ibm.com/">http://www.redbooks.ibm.com/</a> |
| Tivoli Directory Server para z/OS                                              | SG24-7849              | Redbook           | <a href="http://www.redbooks.ibm.com/">http://www.redbooks.ibm.com/</a> |



---

## Glossário

### Ação de Bloqueio

Bloqueia um membro.

### Arquivo de Resposta

1. Um arquivo que contém um conjunto de respostas predefinidas para perguntas feitas por um programa e que é usado para que não seja necessário digitar esses valores um a um.
2. Um arquivo ASCII que pode ser customizado com os dados de definição e de configuração e que automatiza uma instalação. Os dados de definição e de configuração seriam digitados durante uma instalação interativa, mas com um arquivo de resposta a instalação pode prosseguir sem nenhuma intervenção.

### Application Server

1. Um programa que manipula todas as operações do aplicativo entre computadores baseados em navegador e aplicativos ou bancos de dados de negócios de back-end da organização. Essa é uma classe especial de servidores de aplicativos baseados em Java que seguem o padrão Java EE. O código do Java EE pode ser facilmente colocado entre esses servidores de aplicativos. Pode suportar JSPs e servlets para conteúdo da Web dinâmico e EJBs para transações e acesso ao banco de dados.
2. O destino de um pedido de um aplicativo remoto. No ambiente do DB2, a função de servidor de aplicativos é fornecida pelo recurso de dados distribuídos e é utilizada para acessar os dados do DB2 a partir de aplicativos remotos.
3. Um programa do servidor em uma rede distribuída que fornece o ambiente de execução para um programa aplicativo.
4. O destino de um pedido de um solicitador de aplicativo. O sistema de gerenciamento de banco de dados

(DBMS) no site do servidor de aplicativos fornece os dados solicitados.

5. Software que manipula a comunicação com o cliente que está solicitando um recurso e consultas do Content Manager.

### Atributo Bidirecional

Tipo de Texto, Orientação de Texto, Troca Numérica e Troca Simétrica.

### Banco de Dados

Um conjunto de itens de dados inter-relacionados ou independentes que são armazenados para servir um ou mais aplicativos.

### Biblioteca de Carregamento

Uma biblioteca que contém módulos de carregamento.

### Bidirecional (bi-di)

Pertencente a scripts, como Árabe e Hebraico, que geralmente são executados da direita para a esquerda, exceto números, que são executados da esquerda para a direita. Essa definição é do Glossário LISA (Localization Industry Standards Association).

### Buffer de Erro

Uma parte do armazenamento utilizada para conter temporariamente informações de saída de erro.

### Compilar

1. Em linguagens ILE (Integrated Language Environment), para converter instruções de origem em módulos que, então, podem ser ligados a programas ou programas de serviços.
2. Para traduzir todo o programa ou parte dele, expresso em um idioma de alto nível em um programa de computador expresso em uma linguagem intermediária, uma linguagem Assembly ou uma linguagem da máquina.

## Conjunto de Dados

A principal unidade de armazenamento e recuperação de dados, que consiste em um conjunto de dados em uma das muitas organizações prescritas e descritas pelas informações de controle às quais o sistema tem acesso.

## Contêiner

1. No CoOperative Development Environment/400, um objeto de sistema que contém e organiza arquivos de origem. Uma biblioteca i5/OS ou um conjunto de dados particionado por MVS são exemplos e um contêiner.
2. No Java EE, uma entidade que fornece serviços de gerenciamento de ciclo de vida, segurança, implementação e tempo de execução para componentes. (Sun) Cada tipo de contêiner (EJB, Web, JSP, servlet, applet e cliente aplicativo) também fornece serviços específicos ao componente
3. Em Serviços de Recuperação e Mídia de Backup, o objeto físico usado para armazenar e mover mídia, como uma caixa, um estojo ou um rack.
4. Em um servidor de fita virtual (VTS), um receptáculo em que um ou mais volumes lógicos exportados (LVOLs) podem ser armazenados. Um volume temporário que contém um ou mais LVOLs e reside fora de uma biblioteca de VTS é considerado o contêiner para esses volumes.
5. Uma localização do armazenamento físico dos dados. Por exemplo, um arquivo, um diretório ou um dispositivo.
6. Uma coluna ou uma linha que é usada para organizar o layout de um portlet ou outro contêiner em uma página.
7. Um elemento da interface com o usuário que contém objetos. No gerenciador de pastas, um objeto que pode conter outras pastas ou documentos.

## Depurar

Para detectar, diagnosticar e eliminar erros em programas.

## Desinstalação Silenciosa

Um processo de desinstalação que não envia mensagens para o console, mas armazena mensagens e erros em arquivos de log depois que o comando de desinstalação é invocado.

## Gateway

1. Um componente de middleware que faz uma ponte entre a Internet e os ambientes de intranet durante chamadas de serviço da Web.
2. Software que fornece serviços entre os nós de extremidades e o restante do ambiente Tivoli.
3. Um componente de um VoIP (Voice over Internet Protocol) que fornece uma ponte entre o VoIP e ambientes alternados em circuito.
4. Um dispositivo ou um programa usado para conectar redes ou sistemas com diferentes arquiteturas de rede. Os sistemas podem ter diferentes características, como protocolos de comunicação diferentes, arquitetura da rede diferente ou políticas de segurança diferentes; nesse caso, o gateway desempenha a função de tradução e também de conexão.

## Interactive System Productivity Facility (ISPF)

Um programa licenciado IBM que serve como um editor de tela inteira e um gerenciador de diálogos. Utilizado para gravar programas aplicativos, permite gerar painéis de tela padrão e diálogos interativos entre o programador do aplicativo e o usuário terminal. O ISPF consiste em quatro componentes principais: o DM, o PDF, o SCLM e o C/S. O componente DM é o Dialog Manager, que fornece serviços para diálogos e usuários finais. O componente PDF é o Program Development Facility, que fornece serviços para auxiliar o diálogo ou o desenvolvedor de aplicativos. O componente SCLM é o

Software Configuration Library Manager, que fornece serviços para que desenvolvedores de aplicativos gerenciem suas bibliotecas de desenvolvimento de aplicativos. O componente C/S é o Client/Server, que permite executar o ISPF em uma estação de trabalho programável, para exibir os painéis que usam a função de exibição do sistema operacional da estação de trabalho e para integrar ferramentas e dados da estação de trabalho a ferramentas e dados do host.

**ID da Ação**

Um identificador numérico para uma ação entre 0 e 999

**Intérprete**

Um programa que traduz e executa cada instrução de uma linguagem de programação de alto nível antes de traduzir e executar a próxima instrução.

**Isomórfico**

Cada elemento composto (em outras palavras, um elemento contendo outros elementos) do documento da instância XML iniciando a partir da raiz tem um, e apenas um, item do grupo COBOL correspondente cuja profundidade de aninhamento é idêntica à profundidade de aninhamento de seu equivalente XML. Cada elemento não-composto (em outras palavras, um elemento que não contém outros elementos) do documento da instância XML iniciando a partir da parte superior tem um e apenas um item elementar COBOL correspondente cuja profundidade de aninhamento é idêntica ao nível de aninhamento de seu equivalente XML e cujo endereço de memória no tempo de execução pode ser exclusivamente identificado.

**Instalação Silenciosa**

Uma instalação que não envia mensagens para o console, mas armazena mensagens e erros em arquivos de log. Além disso, uma instalação silenciosa pode utilizar arquivos de resposta para entrada de dados.

**Instância do Repositório**

Um projeto ou um componente que existe em um SCM.

**Lista de Tarefas**

Uma lista de procedimentos que podem ser executados por um único fluxo de controle.

**Não isomórfico**

Um mapeamento simples de itens COBOL e elementos XML pertencentes a documentos XML e grupos COBOL que não têm formas idênticas (não-isomórfico). O mapeamento não-isomórfico também pode ser criado entre elementos não-isomórficos de estruturas isomórficas.

**Nome da Shell**

O nome da interface shell.

**Perspectiva**

Um grupo de visualizações que mostram vários aspectos dos recursos do ambiente de trabalho. O usuário do ambiente de trabalho pode alternar perspectivas, dependendo da tarefa disponível, e customizar o layout de visualizações e editores na perspectiva.

**Perspectiva Sistemas Remotos**

Fornece uma interface para gerenciar sistemas remotos utilizando convenções semelhantes a ISPF.

**RAM** Repository Access Manager

**Repositório**

1. Uma área de armazenamento de dados. Cada repositório tem um nome e um tipo de item de negócios associado. Por padrão, o nome será igual ao nome do item de negócios. Por exemplo, um repositório para faturas será chamado Faturas. Há dois

tipos de repositórios de informações: local (específico ao processo) e global (reutilizável).

2. Um conjunto de dados VSAM em que os estados de processos BTS são armazenados. Quando um processo não está sendo executado sob o controle do BTS, seu estado (e os estados de suas atividades constituintes) é preservado com a gravação em um conjunto de dados do repositório. Os estados de todos os processos de um tipo de processo específico (e de suas instâncias de atividade) são armazenados no mesmo conjunto de dados do repositório. Registros de vários tipos de processo podem ser gravados no mesmo repositório.
3. Uma área de armazenamento persistente para código de origem e outros recursos de aplicativo. Em um ambiente de programação em equipe, um repositório compartilhado permite o acesso de multiusuários aos recursos de aplicativo.
4. Um conjunto de informações sobre os gerenciadores de filas que são membros de um cluster. Essas informações incluem nomes de gerenciadores de filas, seus locais, seus canais, quais filas eles hospedam, etc.

### **Script da Shell**

Um arquivo que contém comandos que podem ser interpretados pelo shell. O usuário digita o nome do arquivo de script no prompt do comando shell para fazer com que a shell execute os comandos do script.

**Shell** Uma interface de software entre usuários e o sistema operacional que interpreta comandos e interações com o usuário e comunica-os ao sistema operacional. Um computador pode ter várias camadas de shells para diversos níveis de interação com o usuário.

### **Siddeck**

Uma biblioteca que publica as funções de um programa DLL. Os nomes de entrada e de módulo são armazenados na biblioteca após a compilação do código de origem.

### **Sistema de Arquivo Remoto**

Um sistema de arquivo que reside em um servidor ou sistema operacional separado.

### **Sistema Remoto**

Qualquer outro sistema na rede com o qual o sistema possa se comunicar.

### **Sessão de Depuração**

As atividades de depuração que ocorrem entre o momento em que o desenvolvedor inicia um depurador e o momento em que ele sai dali.

### **Solicitação de Construção**

Um pedido do cliente para executar uma transação de construção.

### **Seção de Ligação**

A seção da divisão de dados de uma unidade ativada (um programa chamado ou um método invocado) que descreve itens de dados disponíveis da unidade de ativação (um programa ou um método). Esses itens de dados podem ser usados como referência tanto pela unidade ativada quanto pela unidade de ativação.

### **Transação de Construção**

Uma tarefa iniciada no MVS para executar construções após um pedido de construção ser recebido do cliente.

**URL** Uniform Resource Locator

### **Visualização Repositórios**

Exibe os locais de repositório CVS que foram incluídos no Ambiente de Trabalho.

### **Visualização Servidores**

Exibe uma lista de todos os servidores e as configurações associadas a eles.

### **Visualização Console de Saída**

Exibe a saída de um processo e permite fornecer entrada do teclado a um processo.

### **Visualização Navegador**

Fornece uma visualização hierárquica dos recursos do Ambiente de Trabalho.

### **Visualização Saída**

Exibe mensagens, parâmetros e resultados relacionados aos objetos com os quais você trabalha

**Visualização Definição de Dados**

Contém uma representação local de bancos de dados e seus objetos e fornece recursos para manipular esses objetos e exportá-los para um banco de dados remoto





---

## Avisos

© Copyright IBM Corporation 1992, 2013.

Direitos Restritos para Usuários do Governo dos Estados Unidos - Uso, duplicação ou divulgação restritos pelo documento GSA ADP Schedule Contract com a IBM Corp.

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante IBM local para obter informações sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não IBM são de responsabilidade do cliente.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não lhe garante direito algum sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:

*Gerência de Relações Comerciais e Industriais da IBM Brasil  
IBM Brasil - Centro de Traduções  
Botafogo  
Rio de Janeiro, RJ  
CEP 22290-240*

Para consultas sobre licença relacionadas a informações de DBCS (Conjunto de Caracteres de Byte Duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie consultas, por escrito, para:

*Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan, Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokyo 103-8510, Japan*

**O parágrafo a seguir não se aplica a nenhum país em que tais disposições não estejam de acordo com a legislação local:** A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS DE NÃO INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, essa disposição pode não se aplicar ao Cliente.

Essas informações podem conter imprecisões técnicas ou erros tipográficos. Periodicamente, são feitas alterações nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Referências nestas informações a websites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses websites. Os materiais contidos nesses websites não fazem parte dos materiais desse produto IBM e a utilização desses websites é de inteira responsabilidade do Cliente.

A IBM pode utilizar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

Portadores de Licenças deste programa que desejarem ter informações sobre ele com a finalidade de: (i) troca de informações entre programas criados de forma independente de outros programas (inclusive este) e (ii) o uso mútuo de informações trocadas, deverão entrar em contato com:

.  
*Intellectual Property Dept. for Rational Software*  
*IBM Brasil - Centro de Traduções*  
*Silicon Valley Lab*  
*555 Bailey Avenue*  
*San Jose, CA 95141-1003*  
*CEP 22290-240*

Estas informações podem estar disponíveis, sujeitas a termos e condições apropriados, incluindo, em alguns casos, o pagamento de uma taxa.

O programa licenciado descrito nesta publicação e todo o material licenciado disponível são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, do Contrato Internacional de Licença do Programa IBM ou de qualquer outro contrato equivalente.

Todos os dados de desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais podem variar significativamente. Algumas medidas podem ter sido tomadas em sistemas em nível de desenvolvimento e não há garantia de que essas medidas serão iguais nos sistemas geralmente disponíveis. Além disso, algumas medidas podem ter sido estimadas por extrapolação. Os resultados reais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

As informações relativas a produtos não IBM foram obtidas dos fornecedores desses produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou estes produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não IBM. As dúvidas sobre os recursos de produtos não IBM devem ser encaminhadas aos fornecedores desses produtos.

Todas as declarações sobre futura direção ou intenção da IBM estão sujeitas a mudança ou retirada, e representam apenas metas e objetivos.

Estas informações contêm exemplos de dados e relatórios utilizados em operações de negócios diárias. Para ilustrá-los da forma mais completa possível, os exemplos incluem nomes de pessoas, empresas, marcas e produtos. Todos esses nomes são fictícios e qualquer semelhança com nomes e endereços usados por uma empresa real terá sido mera coincidência.

## **Licença de Copyright**

Estas informações contêm programas de aplicativos de amostra na linguagem fonte, ilustrando as técnicas de programação em diversas plataformas operacionais. O Cliente pode copiar, modificar e distribuir estes programas de amostra sem a necessidade de pagar à IBM, com objetivos de desenvolvimento, utilização, marketing ou distribuição de programas aplicativos em conformidade com a interface de programação de aplicativo para a plataforma operacional para a qual os programas de amostra são criados. Esses exemplos não foram minuciosamente testados sob todas as condições. Portanto, a IBM não pode garantir ou implicar a confiabilidade, manutenção ou função destes programas. Os programas de amostra são fornecidos "NO ESTADO EM QUE SE ENCONTRAM", sem garantia de nenhum tipo. A IBM não é responsável por nenhum dano decorrente do uso dos programas de amostra.

Cada cópia ou parte deste exemplo de programas ou qualquer trabalho derivado deve incluir um aviso de copyright com os dizeres:

© (o nome da sua empresa) (ano). Partes deste código são derivadas dos Programas de Amostras da IBM Corp. © Copyright IBM Corp. 1992, 2013.

Se estas informações estiverem sendo exibidas em cópia eletrônica, as fotografias e ilustrações coloridas podem não aparecer.

## **Considerações sobre Política de Privacidade**

Os produtos de Software IBM, incluindo soluções de software como serviço, ("Ofertas de Software") podem usar cookies ou outras tecnologias para coletar as informações de uso do produto, para ajudar a melhorar a experiência do usuário final, para customizar as interações com o usuário final ou para outros propósitos. Em muitos casos, nenhuma informação pessoalmente identificável é coletada pelas Ofertas de Software. Algumas de nossas Ofertas de Software podem ajudar a permitir que você colete informações pessoais identificáveis. Se esta Oferta de Software usar cookies para coletar informações de identificação pessoal, informações específicas sobre o uso de cookies desta oferta serão estabelecidas a seguir.

Esta Oferta de Software não usa cookies ou outras tecnologias para coletar informações de identificação pessoal.

## **Marcas Registradas**

IBM, o logotipo IBM e [ibm.com](http://ibm.com) são marcas comerciais ou marcas registradas da International Business Machines Corp., registradas em vários países no mundo todo. Outros nomes de produtos e serviços podem ser marcas comerciais da IBM ou de outras empresas. Uma lista atual das marcas comerciais da IBM está disponível na web em "Informações de Copyright e marca comercial" em [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

## **Termos e Condições para Documentação do Produto**

## **Aplicabilidade**

Estes termos e condições adicionam-se a quaisquer termos de uso do website da IBM.

## **Uso pessoal**

É possível reproduzir essas publicações para uso pessoal não comercial, desde que todos os avisos do proprietário sejam preservados. O cliente não pode distribuir, exibir ou fazer trabalho derivado destas publicações ou de qualquer parte delas sem o expreso consentimento da IBM.

## **Uso comercial**

O cliente pode reproduzir, distribuir e exibir essas publicações unicamente dentro de sua empresa, contanto que todos os avisos do proprietário sejam preservados. O Cliente não pode criar trabalhos derivativos destas publicações ou reproduzir, distribuir ou exibir estas publicações, ou qualquer parte delas, fora de sua empresa, sem o consentimento expreso da IBM.

## **Direitos**

Exceto quando concedido expressamente nesta permissão, nenhuma outra permissão, licença ou direito será concedida, seja de maneira expressa ou implícita, para as publicações ou quaisquer informações, dados ou software ou outra propriedade intelectual nela contida.

A IBM reserva-se o direito de anular as permissões concedidas aqui sempre que, a seu critério, o uso das publicações seja prejudicial para seu interesse ou, conforme determinado pela IBM, as instruções citadas anteriormente não estejam sendo adequadamente seguidas.

O Cliente não pode fazer download, exportar ou reexportar estas informações, exceto em conformidade total com todas as leis e regulamentações aplicáveis, incluindo todas as leis e regulamentações de exportação nos Estados Unidos.

A IBM NÃO OFERECE NENHUMA GARANTIA QUANTO AO CONTEÚDO DESTAS PUBLICAÇÕES. AS PUBLICAÇÕES SÃO FORNECIDAS “NO ESTADO EM QUE SE ENCONTRAM” E SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS DE NÃO INFRAÇÃO, COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO.

---

## **Licença de Copyright**

Estas informações contêm programas de aplicativos de amostra na linguagem fonte, ilustrando as técnicas de programação em diversas plataformas operacionais. O Cliente pode copiar, modificar e distribuir estes programas de exemplo sem a necessidade de pagar à IBM, com objetivos de desenvolvimento, utilização, marketing ou distribuição de programas aplicativos em conformidade com a interface de programação de aplicativo para a plataforma operacional para a qual os programas de exemplo são criados. Esses exemplos não foram testados completamente em todas as condições. Portanto, a IBM não pode garantir ou implicar a confiabilidade, manutenção ou função destes programas. Os programas

de amostra são fornecidos "NO ESTADO EM QUE SE ENCONTRAM", sem garantia de nenhum tipo. A IBM não é responsável por nenhum dano decorrente do uso dos programas de amostra.

---

## Reconhecimentos de Marca Registrada

IBM, o logotipo IBM e [ibm.com](http://ibm.com) são marcas ou marcas registradas da International Business Machines Corp., registradas em vários países no mundo todo. Outros nomes de produtos e serviços podem ser marcas registradas da IBM ou de outras empresas. Uma lista atual de marcas registradas da IBM está disponível na Web em [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Adobe e PostScript são marcas comerciais da Adobe Systems Incorporated.

Cell Broadband Engine - Sony Computer Entertainment Inc.

Rational é uma marca comercial da International Business Machines Corporation e do Rational Software Corporation, nos Estados Unidos, em outros países ou em ambos.

Intel, Intel Centrino, Intel SpeedStep, Intel Xeon, Celeron, Itanium, e Pentium são marcas comerciais da Intel Corporation nos Estados Unidos, em outros países ou em ambos.

IT Infrastructure Library é uma marca comercial da Central Computer and Telecommunications Agency

ITIL é uma marca comercial do The Minister for the Cabinet Office

Linear Tape-Open, LTO e Ultrium são marcas comerciais de HP, IBM Corp. e Quantum

Linux são marcas comerciais do Linus Torvalds

Microsoft, Windows e o logotipo Windows são marcas ou marcas registradas da Microsoft Corporation nos Estados Unidos e/ou em outros países.

Java e todas as marcas registradas e logotipos baseados em Java são marcas ou marcas registradas da Sun Microsystems, Inc. nos Estados Unidos e em outros países.

UNIX é uma marca registrada do The Open Group nos Estados Unidos e em outros países.





---

# Índice

## Caracteres Especiais

.dstoreMemLogging 164  
.dstoreTrace 164  
\_RSE\_PORTRANGE 22  
/var/rdz/pushtoclient/\*install 131, 134

## A

ACEE, gerenciado 41  
acesso ao depurador integrado,  
Definir 54  
acesso às bibliotecas do sistema,  
Aprimorar o 113  
Acesso condicional a arquivos em  
spool 29  
ACK, atrasado 64  
ACK atrasado 64  
Ações condicionais em tarefas 26  
Ações nas Tarefas - Limitações de  
Execução 27  
administradores que não são do sistema,  
privilégios de atualização 17  
administrative utility, notas de  
migração 144  
administrative utility administradores  
CICS  
funções fornecidas 141  
ADNJSPAU, Administrative utility 141  
ajustando considerações 79  
ambiente de linguagem, Bibliotecas de  
tempo de execução do 114  
ambiente TSO, Customizando 153  
ambiente UNIX, Ordens de procura  
usadas no 204  
ambiente z/OS UNIX, Ordens de procura  
usadas no 204  
Análise de Log e Configuração Usando  
FEKLOGS 163  
análise de uso, armazenamento de  
amostra 96  
anel de chave com o RACF, Criar  
um 185  
APF, autorização 176  
aplicativo, Desenvolvimento do 114  
Application Deployment Manager,  
customizando 137  
Application Deployment Manager, editor  
de Definição de Recurso CICS 137  
Application Deployment Manager,  
servidor de Definição de Recurso  
CICS 137  
Aprimorando o desempenho da  
verificação de segurança 115  
Aprimorar o acesso às bibliotecas do  
sistema 113  
AQEZPCM 21  
armazenamento de chaves com keytool,  
Criar um 193  
armazenamento de uso, análise de  
uso 96  
armazenamento em cache, ACEE 42  
Armazenamento em cache do ACEE 42  
arquivos controlados pelo programa  
UNIX para RSE, Definir 52  
arquivos controlados pelo programa  
z/OS UNIX para RSE, Definir 52  
Arquivos de Base da Configuração do  
Resolvedor 205  
arquivos de configuração, Developer for  
System z 42  
Arquivos de configuração, níveis de  
software idênticos, diferentes 158  
arquivos de configuração, Resolvedor de  
base 205  
arquivos de configuração diferentes com  
níveis de software idênticos 158  
Arquivos de dump 170  
arquivos de log  
.dstoreMemLogging 164  
.dstoreTrace 164  
audit.log 164  
fa.log 164  
fekfivpi.log 164  
fekfivps.log 164  
ffs.log 164  
ffsget.log 164  
ffsput.log 164  
lock.log 164  
rmt\_class\_loader.cache.jar 164  
rsecomm.log 164  
rsedaemon.log 164  
rseserver.log 164  
serverlogs.count 164  
stderr.log 164  
stdout.log 164  
arquivos de log do conjunto de  
encadeamentos RSE  
audit.log 166  
rsedaemon.log 166  
rseserver.log 166  
serverlogs.count 166  
stderr.\*.log 166  
stdout.\*.log 166  
arquivos de log do daemon RSE  
audit.log 166  
rsedaemon.log 166  
rseserver.log 166  
serverlogs.count 166  
stderr.\*.log 166  
stdout.\*.log 166  
arquivos em spool, Acesso condicional  
a 29  
arquivos ISPF.conf, utilizar com várias  
configurações 155  
ASCHPMxx  
MAX 105  
ASSIZEMAX 48  
ativação 123  
Ativação da Política AT-TLS 201

ativação da saída de usuário 149  
ativar compartilhamento de classe, Java  
Virtual Machines (JVMs) 116  
atributo do sistema de arquivos,  
SETUID 175  
atributo do sistema de arquivos  
SETUID 175  
Atualizações de Segurança do  
AT-TLS 199  
audit.action, saída de usuário 151  
audit.log 165  
autenticação, Configurando SSL e  
X.509 183  
autenticação, Debug Manager 21  
autenticação, JES Job Monitor 20  
Autenticação de cliente usando  
certificados X.509 31  
autenticação do Debug Manager 21  
Autenticação do JES Job Monitor 20  
autenticação pelo daemon RSE 34  
autenticação pelo software de  
segurança 33  
autenticação x.509, configurando 183  
Autorização APF  
FEK.SFEKAUTH 54  
Autorização de controle de  
programa 175

## B

backend push-to-client, incluindo no  
LDAP 130  
banco de dados de chaves com  
gskkyman, Criar um 191  
Bibliotecas, tempo de execução, ambiente  
de linguagem 114  
bibliotecas controladas para RSE, Definir  
MVS 49  
bibliotecas controladas pelo programa  
MVS para RSE, Definir 49  
Bibliotecas de tempo de execução do  
ambiente de linguagem 114  
bibliotecas do sistema, Aprimorar o  
acesso às 113  
bibliotecas para RSE, Definir MVS 49  
bits de permissão, z/OS UNIX 174  
Bits de permissão do z/OS UNIX 174  
BPXPRMxx 110  
INADDRANYCOUNT 104  
MAXASSIZE 48, 103, 179  
MAXFILEPROC 103  
MAXMMAPAREA 103  
MAXPROCSYS 101, 180  
MAXPROCUSER 101, 180  
MAXSOCKETS 104  
MAXTHREADS 101  
MAXTHREADTASKS 101  
MAXUIDS 103, 181

## C

- características da saída de usuário 149
- carga de trabalho, Gerenciamento de 115
- CARMA, Criação de logs do 168
- CEE.SCEELPA
  - SYS1.PARMLIB(LPALSTxx) 114
- certificado, X.509 20
- Certificado X.509 20
- certificado X.509 e terceira parte 20
- certificados, autenticação de cliente usando X.509 31
- certificados X.509, usando autenticação de cliente 31
- Certificate Revocation List (CRL), consultando
  - rsed.envvars 32
  - variáveis de ambiente do CRL 32
- chaves privadas e certificados, decidir onde armazenar 184
- CICSplex SM Business Application Services (BAS) 138
- classes de segurança, Ativar configurações e 46
- classificação de carga de trabalho, WLM 71
- CLASSPATH 158
- Client Gateway, Usando o método de acesso do TSO/ISPF 154
- clonando configuração RSE existente 186
- COBOL
  - verificação remota 174
- coexistência, atualizar rsed.envvars para ativar a coexistência 187
- comandos de segurança, úteis
  - ADDGROUP 17
  - ALTUSER 17
  - CONNECT 17
- comandos do z/OS UNIX, úteis
  - chgrp 17
  - chmod 17
  - chown 17
  - ls 17
- compartilhamento de classe, ativando em Java Virtual Machines (JVMs) 116
- compartilhamento de classe entre Java Virtual Machines (JVMs) 116
- comportamento TCP/IP, substituindo o padrão 64
- comportamento TCP/IP padrão, substituindo 64
- comunicação, criptografada por SSL 140
- comunicação, criptografada por SSL/TLS 29
- comunicação, Externa 62
- comunicação criptografada
  - Depurador Integrado 31
- comunicação criptografada, SSL 41, 140
- comunicação criptografada, SSL/TLS 29
- comunicação criptografada de SSL/TLS 29
- comunicação criptografada por SSL 41, 140
- Comunicação Externa 62
- comunicação externa para portas especificadas, limitando 22
- Comunicação interna 62
- concatenações de grupo 124
- conexão, Segurança de 21
- conexão da configuração do host Secure Socket Layer, Testar 188
- conexão da configuração do host SSL, Testar 188
- Conexão do Host, Emulador de 181
- conexão recusada 180
- Conexão recusada 180
- configuração, idêntica em um sysplex 157
- configuração de amostra 109
  - contagem do conjunto de encadeamentos 109
  - definindo limites 110
  - determinando limites mínimos 109
- configuração de amostra, seleção de grupo baseada em SAF 133
- configuração de amostra, seleção de grupo LDAP 129
- configuração de grupo LDAP, inicial 130
- configuração de grupo LDAP inicial 130
- Configuração do AT-TLS 195
- configuração do AT-TLS, PROFILE.TCPIP 196
- configuração do JES Job Monitor GEN\_CONSOLE\_NAME 28
- Configuração do Policy Agent 197
- configuração do syslogd 196
- Configuração idêntica em um sysplex 157
- configuração RSE existente, Clonar a 186
- configurações de segurança, verificar 58
- configurações e classes de segurança, Ativar 46
- configurando objetivos, WLM 73
- considerações, Segurança 19
- considerações CICS TS 137
- considerações da saída de usuário xv, 149
- Considerações de LDAP 63
- considerações de push-to-client 119
- Considerações de segurança 19
- Considerações sobre Desempenho 113
- Considerações sobre o TLS v1.2 199
- Considerações WLM xv, 71
- consultar uma Certificate Revocation List (CRL)
  - rsed.envvars 32
  - variáveis de ambiente do CRL 32
- Contagem de encadeamentos 86, 90
- Contagem de processos 83
- Contagem do espaço de endereço 81
- controle de auditoria
  - \_RSE\_HOST\_CODEPAGE 24
  - audit.\* options 24
  - daemon.log 24
  - enable.audit.log 24
- Controle de Configuração do Cliente 122
- Controle de Versão do Cliente 123
- criação de log, cobertura de código 169
- criação de log, conjunto de encadeamento 166
- criação de log, daemon RSE 166
- criação de log, Debug Manager 166
- criação de log, revisão de código 169
- criação de log, SCLM Developer Toolkit 168
- Criação de log, teste IVP do fekfivpi 169
- criação de log da cobertura de código 169
- criação de log da revisão de código 169
- criação de log de auditoria, gerenciado pelo daemon RSE 24
- criação de log de auditoria e daemon RSE 24
- criação de log de instalação de recurso, CICS 139
- criação de log de teste, fekfivpc do IVP 169
- Criação de log de teste, IVP do fekfivpi 169
- Criação de log de teste IVP
  - fekfivpi.log 169
  - fekfivps.log 169
- Criação de log de teste IVP do fekfivpi
  - fekfivpi.log 169
- criação de log do conjunto de encadeamento 166
- criação de log do daemon RSE 166
- Criação de log do Debug Manager 166
- criação de log do SCLM Developer Toolkit
  - rsecomm.log 168
- Criação de Log IVP fekfivpc
  - fekfivpc.log 169
- criação de logs, JES Job Monitor 166
- criação de logs, usuário do RSE 167
- Criação de logs do CARMA
  - rsecomm.log 168
- Criação de logs do Common Access Repository Manager 168
- criação de logs do JES Job Monitor 166
- criação de logs do usuário, RSE 167
- criação de logs do usuário do RSE
  - .dstoreMemLogging 167
  - .dstoreTrace 167
  - ffs.log 167
  - ffsget.log 167
  - ffsput.log 167
  - lock.log 167
  - rmt\_class\_loader.cache.jar 167
  - rsecomm.log 167
  - stderr.log 167
  - stdout.log 167
- criptografia, SSL ou TLS 184
- Criptografia de comunicação usando SSL 22
- Criptografia de comunicação usando TLS 22
- criptografia usando TLS,
  - Comunicação 22
- customização - ISPF.conf, 154
- Customizando o Ambiente TSO 153
- customizando o Application Deployment Manager 137

## D

- dados de auditoria
  - log de ações 25

- Daemon de bloqueio 13
- Daemon em bloqueio (LOCKD) 4
- Daemon RSE 62
- daemon RSE, autenticação pelo 34
- daemon RSE (RSED) 4
- definição de segurança 133
- definições, Segurança 44
- definições de recurso, várias 104
- definições de recurso chave 100
  - r sed.envvars 100
  - SYS1.PARMLIB(BPXPRMxx) 101
- definições de recursos CICS, administrador 137
- definições de recursos CICS, desenvolvedor 137
- Definições de segurança 44
- definições de segurança, Lista de verificação 45
- Definições disponíveis para o resolvidor 208
- Definições locais disponíveis para o resolvidor 208
- Definir acesso para depurador integrado 54
- Definir arquivos controlados pelo programa z/OS UNIX para RSE 52
- Definir bibliotecas controladas pelo programa MVS para RSE 49
- Definir permissão de acesso do arquivo z/OS UNIX para RSE 51
- Definir servidor RSE como um z/OS UNIX seguro 48
- Definir suporte PassTicket para RSE 50
- Definir verificação de Port Of Entry para RSE 34
- Dependência do nome do host 203
- depuração, transação do CICS 147
- depuração de transação do CICS 147
- depurador, integrado 10
- depurador integrado 10
- Depurador Integrado
  - comunicação criptografada 31
- desempenho, Considerações sobre 113
- desempenho da verificação de segurança, Aprimorando o 115
- Desenvolvimento de Aplicativos 114
- Developer for System z, entendimento 3
- Developer for System z, visão geral do componente
  - representação gráfica 3
- Developer for System z tarefa iniciada, Definir 47
- Distributed Dynamic VIPA
  - EZBEPOR T 65
  - PORT 65
  - PORTRANGE 65
  - SERVERWLM 65
  - SYSPLEXPORTS 65
  - VIPADISTRIBUTE 65
- Diversos Grupos de
  - Desenvolvedores 123
- donos das tarefas 6
- Dumps de Java 170
- Dumps do MVS 170

## E

- Editor de Definição de Recurso CICS (CRD), Application Deployment Manager 137
- Emulador de Conexão do Host 181
- endereço do host não resolvido, TCP/IP Resolver
  - lock.log 208
- entendendo o Developer for System z 3
- erro, Rastreo de feedback de 173
- erro de falta de memória 181
- espaço de endereço, Tamanho do 179
- Espaço em disco, Java Virtual Machines (JVMs) 118
- específicas, limitar comunicação externa para portas 22
- Esquema LDAP 128
- estimativa de tamanho, diretrizes 95
- estrutura do diretório, z/OS UNIX
  - representação gráfica 15
- estrutura do diretório z/OS UNIX
  - representação gráfica 15
- etapas de configuração 126
- exec de alocação, usando 155
- Executando várias instâncias 157

## F

- fa.log 164
- feedback de erro, Rastreo de 173
- FEJJC NFG 62, 110, 160
  - CONSOLE\_NAME 27
  - MAX\_THREADS 104
- FEJJC NFG, JES Job Monitor 42
- FEKAPPL 20
- fekfivpc.log 165
- fekfivpi.log 165
- fekfivpi.log, criação de log de teste IVP 169
- fekfivps.log 165
- fekfivps.log, criação de log de teste IVP 169
- FEKLOGS, análise de log e de configuração usando 163
- FEKRACE, definições de segurança 44
- fekrivp 176
- ffs.log 164
- ffsget.log 164
- ffsput.log 164
- Fluxo de conexão 8
  - representação gráfica 8
- Fluxo do daemon de bloqueio
  - representação gráfica 13
- funções de cliente, alterando 35

## G

- GATE, lixeira 41
- Gerenciador de Implementação do Aplicativo (ADM) 4
- Gerenciamento de carga de trabalho 115
- grupos LDAP, incluindo desenvolvedores 131
- gskkyman, Criar um banco de dados de chaves com 191

## H

- heap Java fixo, Tamanho de 115

## I

- ID do usuário, variável, executando com 150
- ID do usuário da variável, executando com 150
- ID do usuário e passphrase 20
- ID do Usuário e Senha 20
- ID do Usuário e Senha Única 20
- IEASYSxx 111
  - MAXUSER 105, 181
- informações de configuração, ordens de procura das 204
- iniciação rápida, opção Java (-Xquickstart) 116
- inicialização, Requisitos da JCL de 179
- Instalação do SMP/E, sticky bit 177
- interface de serviço da Web 138
- interface RESTful 138
- interface RESTful versus interface de serviço da Web 138
- interna, Comunicação 62
- introdução, considerações de push-to-client 119
- ISP.SISPLOAD
  - ISPF TSO/ISPF Client Gateway 49
- ISPF, Usar vários execs de alocação 155
- ISPF.conf, Customização básica 154
- ISPF TSO/ISPF Client Gateway
  - ISP.SISPLOAD 49
- IVTPRMxx
  - ECSA MAX 105
  - FIXED MAX 105

## J

- Java, Dumps de 170
- JAVA\_DUMP\_TDUMP\_PATTERN 171
- Java Virtual Machines (JVMs), compartilhamento de classe entre 116
- JCL de inicialização, Requisitos de 179
- JES JMON
  - GEN\_CONSOLE\_NAME 28
- JES Job Monitor, FEJJC NFG 42
- JES Job Monitor (JMON) 4
- JMON 53, 160
- JVMs, compartilhamento de classe entre 116

## K

- keytool, Criar um armazenamento de chaves com 193

## L

- liberando um bloqueio
  - RSE, comando cancelar modify 14
- ligação da área de trabalho 124
- LIMIT\_COMMANDS 27
- LIMIT\_VIEW 29

- limitações de execução, Ações nas tarefas 27
- limitando comunicação externa, portas específicas 22
- limite de tamanho, espaço de endereço 94
- limite de tamanho, heap Java 93
- Limite de Tamanho de Heap Java 93
- limite de tamanho do espaço de endereço 94
- limite do tamanho de heap, Java 93
- limites de tamanho do cache, Java Virtual Machines (JVMs) 117
- Limites do sistema 180
- Locais do dump, z/OS UNIX 171
- Locais do dump do UNIX 171
- Locais do dump do z/OS UNIX 171
- local de metadados 120
- local de metadados do grupo 125
- local do servidor, LDAP 129
- Local do Servidor LDAP 129
- lock.log 164
- Log de Instalação do Recurso do CICS 139
- logon.action, saída de usuário 152
- LPALSTxx 114

## M

- mensagens, administrative utility 145
- mensagens do administrative utility 145
- mensagens do console, saída de usuário 150
- metadados, push-to-client 120
- metadados push-to-client 120
- método de acesso do TSO/ISPF Client Gateway, Usando o 154
- métodos, Autenticação 20
- Métodos de acesso, TSO 153
- Métodos de acesso do TSO 153
- Métodos de autenticação 20
- monitorando, rede 108
- monitorando o RSE 106
- monitorando z/OS sistema de arquivo UNIX 108
- monitorando z/OS UNIX 107
- MVS, Dumps do 170

## N

- netstat 177
- níveis de software idênticos com arquivos de configuração diferentes 158
- nível de software, idênticos em arquivos de configuração diferentes 158
- nome do host, Dependência do 203
- nomes de host, aplicando no Developer for System z 206
- notas de migração, administrative utility 144

## O

- objetivos, configurando em WLM 73
- OFF.REMOTECOPY.MVS 36

- onde armazenar chaves privadas e certificados 184
- opção Xquickstart Java 116
- Ordens de procura, ambiente z/OS UNIX 204
- ordens de procura das informações de configuração 204
- OutOfMemoryError 181

## P

- passphrase e ID do Usuário 20
- PassTickets, usando 23
- perfil de segurança, Limitações armazenadas no 179
- perfis, Definir conjunto de dados 54
- perfis do conjunto de dados, Definir 54
- perfis do ISPF, Usar existentes 154
- período de carência, rejeitando mudanças 134
- Permissão de acesso do arquivo z/OS UNIX, Definir para RSE 51
- permissão do perfil, BPX.SUPERUSER 39
- Permissão do perfil BPX.SUPERUSER 39
- permissões de classe, UNIXPRIV 39
- Permissões de classe UNIXPRIV 39
- Política AT-TLS 197
- pontos de saída, disponíveis 151
- pontos de saída de usuário, disponíveis 151
- portas, CARMA e TCP/IP 63
- portas, TCP/IP 61
- portas do CARMA e TCP/IP 63
- Portas TCP/IP 61
- portas TCP/IP, representação gráfica 61
- Portas TCP/IP reservadas 177
- PORTRANGE 178
- privilegios de atualização, administradores que não são do sistema 17
- problemas de configuração, Resolução de problemas 163
- processamento de auditoria modify switch 25
- PROFILE.TCPIP, configuração do AT-TLS 196
- projetos, baseados em host 135
- projetos baseados em host 135
- proteção de aplicativo para RSE, Definir 51
- Publicações Referenciadas 211
- push-to-client 36
- pushtoclient.properties 131, 134

## R

- RACF
  - permite 55
- RACE, Criar um anel de chave com o 185
- rastreio 172
- rastreio, CARMA 173
- rastreio, JES Job Monitor 172
- rastreio, RSE 172
- rastreio CARMA 173

- Rastreio de feedback de erro 173
- rastreio do JES Job Monitor 172
- rastreio RSE 172
- reconhecimento, atrasado 64
- recurso do CICS, criação de log de instalação de 139
- rede, monitorando 108
- Referenciadas, publicações 211
- regiões de conexão, primária versus não primária 138
- regiões de conexão primária versus não primária 138
- regras de classificação, WLM 72
- regras de classificação WLM 72
- rejeitando mudanças, período de carência 134
- repositório do CRD 40
- Requisitos da JCL de inicialização 179
- reserva, porta TCPIP 63
- reserva de porta, TCP/IP 63
- Reserva de Porta TCP/IP 63
- reservadas, Portas TCP/IP 177
- Resolução de problemas de configuração 163
- resolvedor, Definições locais disponíveis para o 208
- resolvedores, Compreendendo os 203
- REXX exec do z/OS UNIX 151
- rmt\_class\_loader\_cache.jar 164
- rotina de saída do usuário, gravando 149
- RSE , Definir bibliotecas controladas pelo programa MVS para 49
- RSE , Definir suporte PassTicket para 50
- RSE , Definir verificação de Port Of Entry para 34
- RSE, Definir arquivos controlados pelo programa z/OS UNIX para 52
- RSE, Definir como um servidor z/OS UNIX seguro 48
- RSE, Definir permissão de acesso do arquivo z/OS UNIX 51
- RSE, definir proteção de aplicativo para 51
- RSE, monitorando 106
- RSE, pushtoclient.properties 44
- RSE, rsed.envvars
  - \_RSE\_JAVAOPTS 42
- RSE, ssl.properties 44
- RSE como um Aplicativo Java
  - representação gráfica 5
- rsecomm.log 164
- criação de log do SCLM Developer Toolkit 168
- rsecomm.properties 173
- rsed.envvars 99, 131, 134, 158
  - \_CMDSEV\_CONF\_HOME 156
  - \_RSE\_JAVAOPTS 153, 170
  - \_RSE\_PORTRANGE 22
  - Dmaximum.clients 101
  - Dmaximum.threadpool.process 101
  - Dmaximum.threads 101
  - Dminimum.threadpool.process 101
  - DSTORE\_LOG\_DIRECTORY 168, 172
  - STEPLIB 30
  - Xms 101
  - Xmx 101



rsed.envvars, atualizar para ativar a  
coexistência 187  
rsedaemon.log 164, 165  
rseserver.log 164, 165

## S

saída de usuário, mensagens do  
console 150  
saídas do sistema, Limitações importas  
por 179  
SCLM Developer Toolkit 49  
SCLM Developer Toolkit (SCLMDT) 4  
Secure Socket Layer, Configurando 183  
Secure Socket Layer, Criptografia de  
comunicação usando 22  
segmento, Definir OMVS 47  
segmento OMVS, Definir 47  
segurança, Application Deployment  
Manager (ADM) 139  
segurança, arquivo de log 37  
segurança, CICSTS 40  
segurança, Definir comando do JES 52  
segurança, depuração 40  
segurança, JES 26  
segurança, pipeline 139  
segurança, recurso 141  
segurança, SCLM 41  
segurança, transação 139  
segurança de comando, Definir JES 52  
Segurança de comando do JES,  
Definir 52  
Segurança de conexão 21  
segurança de depuração 40  
segurança de encadeamento no servidor  
RSE  
PassTickets 23  
segurança de metadados 121  
Segurança de Pipeline 139  
Segurança de SCLM 41  
segurança de transação 139  
segurança do Application Deployment  
Manager 139  
segurança do arquivo de log 37  
segurança do cache, Java Virtual  
Machines (JVMs) 117  
segurança do CICSTS 40  
Segurança do JES 26  
segurança do recurso 141  
segurança do repositório, CRD 139  
segurança do repositório CRD 139  
seleção de grupo, baseada em  
LDAP 127  
seleção de grupo, baseada em SAF 132  
seleção de portas, restringindo 67  
seleção do servidor, LDAP 128  
Seleção do Servidor LDAP 128  
senha e ID do usuário 20  
senha única e ID do usuário 20  
serverlogs.count 164  
Serviço TSO Command 4  
serviço TSO Commands 153  
Servidor de Definição de Recurso CICS  
(CRD), Application Deployment  
Manager 137  
Servidor RSE 62  
servidor UNIX, Definir RSE como 48

servidor z/OS UNIX, Definir RSE  
como 48  
servidor z/OS UNIX seguro, Definir RSE  
como um 48  
Shell script do z/OS UNIX 150  
sincronização, automatizada 159  
sincronização automatizada 159  
sistema, Aprimorar o acesso às bibliotecas  
do 113  
sistema, Limites do 180  
sistema primário 120  
sistemas de arquivo zFS, Usando 113  
sistemas de arquivos, zFS 113  
software de segurança, autenticação  
pelo 33  
spool, Acesso condicional a arquivos  
em 29  
SSL, Configurando 183  
SSL, criptografia 184  
SSL, Criptografia de comunicação  
usando 22  
ssl.properties, ativar o SSL criando um  
novo daemon RSE 187  
ssl.properties, Ativar SSL  
atualizando 187  
stderr.\*.log 164  
stderr.log 164  
stdout.\*.log 164  
stdout.log 164  
STEPLIB, Evite o uso de 113  
sticky bit, disponibilidade do módulo de  
carregamento MVS para z/OS  
UNIX 177  
substituindo o comportamento TCP/IP  
padrão 64  
suporte de autenticação de cliente, incluir  
X.509 191  
suporte para RSE, Definir PassTicket 50  
suporte PassTicket para RSE, Definir 50  
SYS1.PARMLIB(BPXPRMxx) 110  
MAXASSIZE 48, 179  
MAXPROCSYS 180  
MAXPROCUSER 180  
MAXUIDS 181  
SYS1.PARMLIB(BPXPRMxx), Java Virtual  
Machines (JVMs) 117  
SYS1.PARMLIB(BPXPRMxx), Limitações  
definidas em 179  
SYS1.PARMLIB(IEASYSxx) 111  
MAXUSER 181  
sysplex, configuração idêntica em 157

## T

tabelas, Conversão 205  
Tabelas, host local 206  
Tabelas de Conversão 205  
Tabelas do host, local 206  
Tabelas do Host Local 206  
Tamanho de heap Java fixo 115  
Tamanho do espaço de endereço 179  
tarefa iniciada, Policy Agent 196  
Tarefa Iniciada do Policy Agent 196  
tarefas, Ações condicionais em 26  
tarefas iniciadas, Definir para Developer  
for System z  
tarefas iniciadas JMON 47

tarefas iniciadas, Definir para Developer  
for System z (*continuação*)  
tarefas iniciadas RSED 47  
TCP/IP, aplicando no Developer for  
System z 206  
TCP/IP, Configurando 203  
TCP/IP, Definições locais disponíveis  
para o resolvidor 208  
TCP/IP reservadas, Portas 177  
TCP/IP Resolver, endereço do host não  
resolvido  
lock.log 208  
Testar a conexão da configuração do host  
SSL 188  
tipos de subsistema  
ASCH 72  
CICS 72  
JES 72  
OMVS 72  
STC 72  
TLS, criptografia 184  
TLS, Criptografia de comunicação  
usando 22  
transações do CICS 41  
TSO/ISPF, customização - ISPF.conf, 154  
TSO/ISPF, Usando um exec de  
alocação 155  
TSO/ISPF, Usar perfis do ISPF  
existentes 154  
TSO/ISPF, Usar vários execs de  
alocação 155  
TSO/ISPF, utilizar com várias  
configurações 155  
TSO/ISPF Client Gateway, Usando o  
método de acesso do 154

## U

UID 0 39  
usando os PassTickets 23  
usando SSL, Criptografia de  
comunicação 22  
Usando um exec de alocação 155  
Usar perfis existentes do ISPF 154  
uso de armazenamento 93  
uso de espaço, metadados 122  
uso de espaço, z/OS UNIX sistema de  
arquivos UNIX 98  
Uso de Espaço de Metadados 122  
Uso de espaço do sistema de arquivos  
z/OS UNIX 98  
uso de recursos, ajustando 79  
uso de recursos, temporário 89  
uso de recursos, visão geral 80  
uso de STEPLIB, Evite o 113  
uso do espaço do sistema de arquivos,  
z/OS UNIX 98  
Uso temporário de recursos 89  
Utilitários do gerenciamento do cache,  
Java Virtual Machines (JVMs) 118

## V

validação da Autoridade de Certificação  
gskkyman 32  
SAF key ring 32

- validação da Autoridade de Certificação  
(*continuação*)
  - TRUST, HIGHTRUST 32
- várias configurações do Developer para  
System z, utilizar vários arquivos  
ISPF.conf com 155
- Várias definições de recurso 104
  - FEJJCNFG 104
  - Placa EXEC, JLC do servidor 104
  - SYS1.PARMLIB(ASCHPMxx) 105
  - SYS1.PARMLIB(IEASYSxx) 105
  - SYS1.PARMLIB(IVTPRMxx) 105
- várias instâncias, Executando 157
- variáveis de padrão de dump de  
transação 171
- Vários arquivos ISPF.conf 155
- vários execs de alocação, TSO/ISPF 155
- verificação de POE 23, 34
- Verificação de Port of Entry 34
- Verificação de Port Of Entry 23
- verificação de segurança, Aprimorando o  
desempenho da 115
- Verificar configurações de segurança 58
- VIPA, Distributed Dynamic 65
- visão geral do componente, Developer for  
System z
  - representação gráfica 3

## W

- Web Owning Region 138
- workload manager 71

## X

- X.509, incluindo suporte de autenticação  
de cliente 191
- Xquickstart, opção Java 116

## Z

- z/OS sistemas de arquivo UNIX,  
monitorando 108
- z/OS UNIX, monitorando 107

---

## Comentários do Leitor

IBM Rational Developer for System z  
Versão 9.1.1  
Guia de Referência de Configuração do Host

Publicação N° SC43-1628-08

Neste formulário, faça-nos saber sua opinião sobre este manual. Utilize-o se encontrar algum erro, ou se quiser externar qualquer opinião a respeito (tal como organização, assunto, aparência...) ou fazer sugestões para melhorá-lo.

Para pedir publicações extras, fazer perguntas ou tecer comentários sobre as funções de produtos ou sistemas IBM, fale com o seu representante IBM.

Quando você envia seus comentários, concede direitos, não exclusivos, à IBM para usá-los ou distribuí-los da maneira que achar conveniente, sem que isso implique em qualquer compromisso ou obrigação para com você.

Não se esqueça de preencher seu nome e seu endereço abaixo, se deseja resposta.

Comentários:

---

Nome

---

Endereço

---

Companhia ou Empresa

---

Telefone



IBM Brasil - Centro de Traduções  
Rodovia SP 101 Km 09  
Hortolândia, SP





Impresso no Brasil

SC43-1628-08

